ГЛАВА 6

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ КОНЕЧНЫХ ТОЧЕК ИНФРАСТРУКТУРНЫХ СИСТЕМ

Рассмотрены особенности решения задачи обеспечения кибербезопасности конечных точек инфраструктурных систем. Конечные точки – это рабочие станции, серверы, ноутбуки. Показано, что даже корпоративные мобильные телефоны для злоумышленников в большинстве случаев являются достаточно простыми и популярными точками проникновения, что повышает значимость контроля за ними со стороны служб кибербезопасности.

Остроту проблемы усугубляет тот очевидный для экспертов факт, что изощренные целевые атаки все чаще применяют сочетание распространенных угроз, детально рассмотренных нами в третьей главе, и уязвимостей нулевого дня, уникальных нестандартных схем – вообще без использования вредоносного программного обеспечения, разнообразных «бесфайловых» методов и т.п.

Присутствующие сегодня в инфраструктурах большинства организаций платформы защиты конечных точек EPP (Endpoint Protection Peatform) отлично защищают от массовых, ранее известных угроз, но они не способны, например, определить, что поступающее предупреждение может быть составными частями более сложной и опасной атаки, которая может повлечь за собой существенный ущерб для организации.

Здесь в качестве примера рассмотрено одно из альтернативных решений – это платформы типа EDR (Endpoint Detection and Response), которые должны автоматически взаимосвязываться с предыдущим поколением EPP.

В этой главе более детально будут рассмотрены тенденции развития киберугроз, направленных именно на конечные точки (в том числе бесфайловых filless-атак), а также технические характеристики и особенности эксплуатации таких основных платформ EDR-решений, как Gamet, Forresher, The Radicati Group.

6.1. Тенденции развития киберугроз, направленных на конечные точки инфраструктурных систем

Все более острой проблемой для многих организаций из различных сфер деятельности становится вероятность столкновения с целенаправленными атаками, которые все чаще применяют сочетание распространенных угроз, уязвимостей нулевого дня, уникальных схем без использования вредоносного программного обеспечения, бесфайловых методов и пр. Использование стандартных решений, построенных на базе превентивных технологий, а также систем, нацеленных точечно на обна-

ружение сложных вредоносных активностей только в сетевом трафике, не может быть достаточным для защиты предприятия от сложносоставных целенаправленных атак. Конечные точки, включая рабочие станции, ноутбуки, серверы и смартфоны, также являются критически важными объектами контроля, так как они остаются для злоумышленников в большинстве случаев достаточно простыми и популярными точками проникновения, что повышает значимость контроля за ними.

Платформы защиты конечных точек (Endpoint Protection Platform – EPP), которые сегодня присутствуют на инфраструктуре у большинства организаций, отлично защищают от массовых, известных, а также и ряда неизвестных угроз, но в большинстве случаев, построенных на базе уже ранее встречающихся вредоносных программ. Со временем техники нападения киберпреступников претерпели значительные изменения. Злоумышленники стали более агрессивны в своих атакующих подходах и более совершенны в организации всех этапов процесса. А потому большое количество компаний, несмотря на использование решений по защите конечных точек (EPP), все же подвергаются компрометации. Это означает, что сегодня организациям уже необходимы дополнительные инструменты, которые помогут им эффективно обнаруживать новейшие, более сложные угрозы, с которыми уже не в состоянии справиться традиционные средства защиты, изначально не разрабатываемые против подобного рода угроз. Эти средства защиты хотя и выявляют инциденты на конечных точках, но обычно не способны определить, что поступающие предупреждения могут быть составными частями более опасной и сложной схемы, которая может повлечь за собой значимый для организации ущерб.

Современная защита конечных точек нуждается в адаптации к современному ландшафту сложных угроз и должна включать функциональность по обнаружению комплексных атак, направленных на конечные точки, и быть способной оперативно реагировать на найденные инциденты (Endpoint Detection and Response – EDR).

Ожидаемым результатом от внедрения EDR-решения по противодействию сложным угрозам будет организация передовой защиты конечных устройств, что приведет к заметному уменьшению поверхности комплексных целевых атак и тем самым к сокращению общего числа киберугроз.

В качественном обзоре [1] рассмотрены базовые технологии EDR и особенности их взаимодействия с решениями класса EPP.

Очевидно, что опубликованная информация об успешно проведенных атаках, направленных на различные государственные и коммерческие организации, – это всего лишь маленькая часть от их реального количества. С уверенностью можно утверждать, что количество киберинцидентов и уровень последствий от них гораздо выше, чем представляется нам в средствах массовой информации.

Например, собранные цифры в ходе глобального исследования рисков информационной безопасности для бизнеса Kaspersky Lab Global Corporate IT Security Risks Survey подтверждают, что успешные кибератаки действительно обходятся дорого компаниям. Для каждой из рассматриваемых категорий затрат были рассчитаны средние потери, которые понесли организации в России, столкнувшиеся с ИБ-инцидентами. А сумма всех категорий позволила оценить среднюю величину общего ущерба, нанесенного успешной атакой, которая составила более 16 миллионов рублей.

Рис. 6.1. Средние затраты компаний, столкнувшихся с ИБ-инцидентами, Kaspersky Lab Global Corporate IT Security Risks Survey, 2017

По данным исследования компании PWC, опубликованным в отчете «Глобальные тенденции информационной безопасности на 2018 год», руководители организаций, использующих системы автоматизации, признали растущую опасность киберугроз и значимость потенциальных негативных последствий от кибератак. В качестве основного возможного результата кибератаки 40% участников опроса в мире и 37% по России назвали нарушение операционной деятельности, 39% – утечку конфиденциальных данных (48% – в России), 32% – причинение вреда качеству продукции (27% – в России).

В наши дни на рынке отмечается новая тенденция современных направленных атак, где злоумышленники в качестве своих жертв выбирают уже не только крупные организации, но и цели поменьше и все чаще используют небольшие организации в цепочке атаки на крупные компании. Злоумышленники становятся более аккуратными к затратам на подготовку атак и стремятся как можно сильнее минимизировать расходы, вследствие чего стоимость организации эффективной целенаправленной атаки значительно снижается, и, соответственно, возрастает и общее количество атак в мире.

Это подтверждает и статистика. По данным международного опроса, проведенного аналитическим агентством B2B International по заказу «Лаборатории Касперского», доля целенаправленных атак в 2017 году выросла на 10% по сравнению с 2016 годом и составила 23%. Это означает, что почти четверть компаний стали жертвами этих атак и почти две трети респондентов (63%) считают, что угрозы, с которыми они столкнулись в 2017 году, стали на порядок сложнее. А 53% компаний считают, что защита их организаций рано или поздно будет взломана. В результате большинство организаций понимают, что невозможно избежать брешей в системах ИБ, и вероятность столкновения с целенаправленной атакой с каждым днем возрастает.

В комплексных атаках, направленных на конкретные организации, применяются: мультивекторный подход к проникновению, поиск уязвимых мест в инфраструктуре, тщательное изучение существующих средств защиты с целью их обхода, использование специально разработанного или модифицированного вредоносного кода, применение социальной инженерии, шифрования и последующей обфускации для исключения вероятности обнаружения.

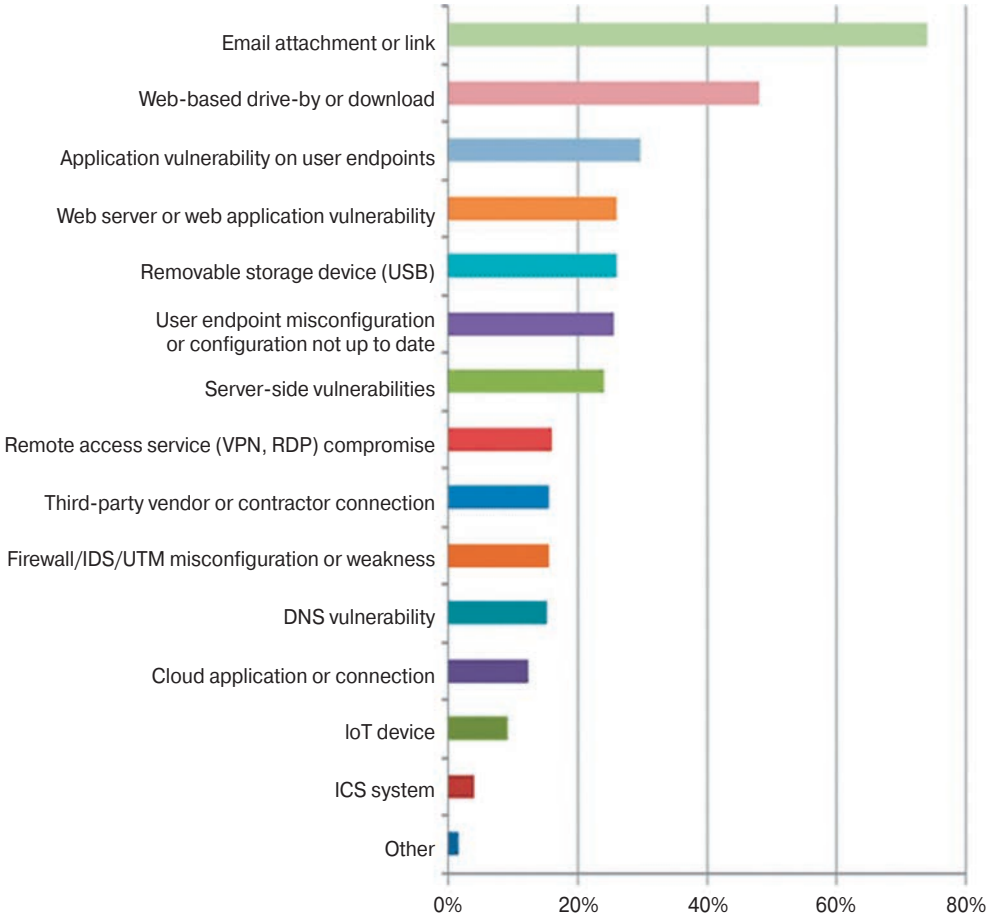

Рис. 6.2. Vectors Threats Use to Enter Organizations, SANS 2017 Threat Landscape Survey: Users on the Front Line

По данным отчета о современном ландшафте угроз SANS 2017 Threat Landscape Survey: Users on the Front Line:

– 74% респондентов назвали одним из распространенных способов проникновения вредоносных объектов в организацию зараженные ссылки в теле электронных писем или исполняемые вредоносные файлы, распространяющиеся в виде вложений;
– 48% респондентов выделили активацию вредоносов с зараженных веб-сайтов или самостоятельную загрузку вредоносных файлов при посещении веб-страниц;
– 30% указали на уязвимости приложений на конечных точках пользователя и др.

По данным этого же отчета, 81% опрошенных компаний считают, что средства по защите конечных точек становятся наиболее востребованными инструментами.

Наблюдая за эволюцией угроз от массовых к направленным, мы видим потребность в добавлении к автоматическому блокированию более простых угроз,

продвинутое обнаружение направленных сложных угроз и в целом перестроения рынка и смене фокуса от защиты отдельных рабочих мест к обеспечению безопасности целого предприятия с привлечением не только специалистов ИТ-департамента, но и специалистов по информационной безопасности и аналитиков для дальнейшего расследования инцидентов, оперативного реагирования и поиска новейших угроз.

Рассмотрим более подробно ключевые тенденции развития угроз, затрагивающие конечные точки сети.

6.2. Тенденция роста бесфайловых (fileless) атак

Бесфайловые атаки – это атаки, которые не размещают никаких файлов на жестком диске. Отследить такого рода активности на порядок сложнее. Злоумышленники могут использовать эксплойты, макросы, скрипты и легитимные инструменты. Можно выделить несколько видов бесфайловых атак:

- размещение в оперативной памяти;
- сохранение в реестре Windows;
- использование доверенного программного обеспечения: инструментов Windows, различных приложений и т.п. для получения учетных данных целевых систем для вредоносных целей;
- атаки с использованием скриптов.

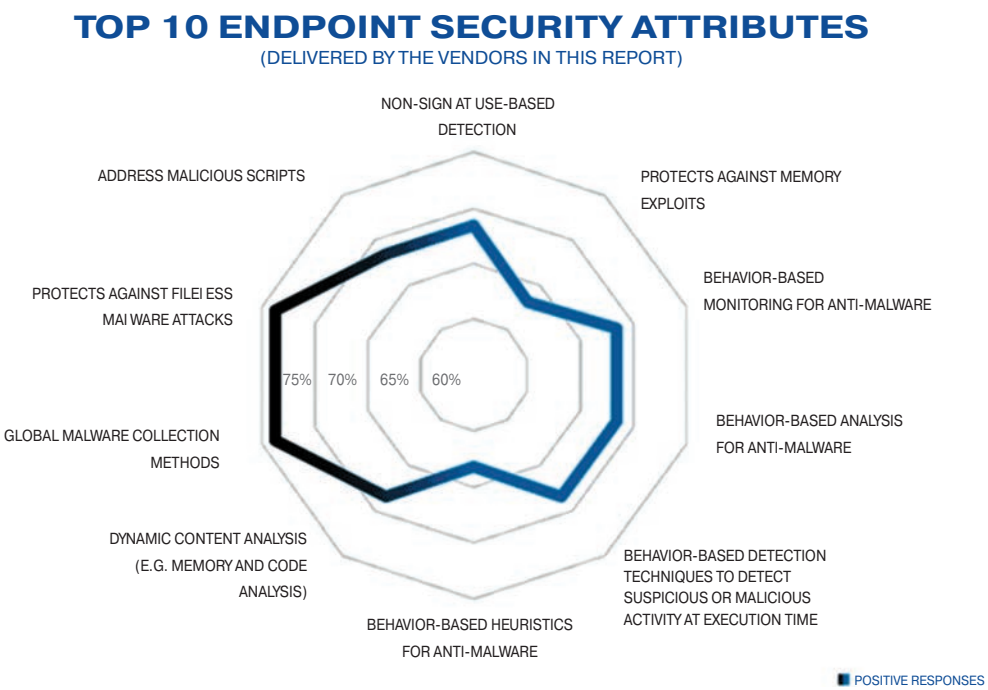

Рис. 6.3. Top 10 Endpoint security attributes, CISOs Investigate: Endpoint Security by Security Current, 2017

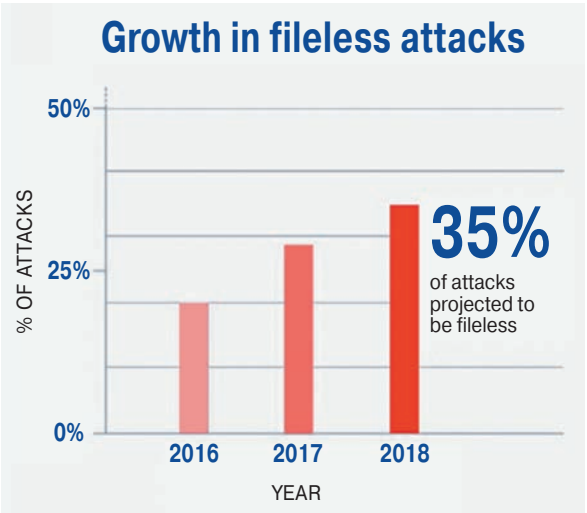

Рис. 6.4. График роста бесфайловых атак, New Ponemon Institute, 2017

С каждым годом вероятность столкновения с направленными атаками на конечных точках для организаций увеличивается. Вместо установки вредоносных исполняемых файлов, которые антивирусные движки могут без проблем оперативно находить и блокировать, злоумышленники используют различные комбинации с применением бесфайловых методов, заражая конечные точки и не оставляя при этом артефактов, которые можно было бы обнаружить в ста процентах случаев антивирусом.

Опрос CISOs Investigate: Endpoint Security by Security Current, в котором были включены отзывы руководителей по информационной безопасности, которые уже используют решения по продвинутой защите конечных точек или только планируют, а также ответы проанкетированных производителей этих решений показали, что противодействие бесфайловым атакам на конечных точках является одним из главных атрибутов информационной безопасности, на который стоит обратить особое внимание.

По данным опрошенных организаций, 29% нападений, с которыми они столкнулись в течение 2017 года, были бесфайловыми, что на 9% больше, чем годом ранее. New Ponemon Institute еще в 2017 г. прогнозировало, что эта пропорция продолжит расти, и в 2018 г. бесфайловые атаки составят 35% от общего количества всех прогнозируемых атак. На момент выхода книги можно сказать, что этот прогноз полностью подтвердился.

6.3. Рост ущерба от атак на конечные точки

Исходя из цифр, которые предоставляет нам New Ponemon Institute, в среднем за 2017 год компании потеряли из-за успешных атак, в которых злоумышленники обошли существующие системы безопасности конечных точек, в общей сложности более 5 миллионов долларов (средняя стоимость 301 доллар США на одного сотрудника), что является значительной цифрой и говорит о том, что современные компании нуждаются в пересмотре своей стратегии защиты конечных точек.

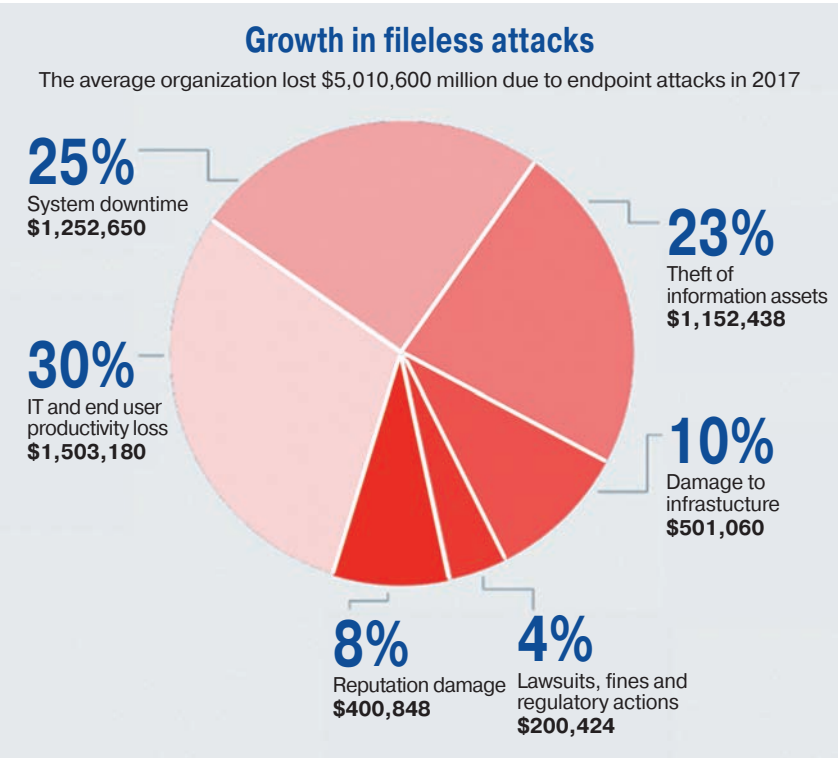

Рис. 6.5. Стоимость атак на конечные точки сети, New Ponemon Institute, 2017

6.4. Мировой рынок EDR-решений

Несмотря на популярность традиционных средств защиты конечных точек, многие организации тем не менее рассматривают и добавляют новые технологические возможности поверх своих EPP-решений, чтобы повысить качество обнаружения сложных угроз и ускорить процесс реагирования на них, уменьшая тем самым вероятность возникновения успешных атак и разрушительного влияния на бизнес.

Как мы видим, в обеспечении безопасности конечных точек на рынке присутствуют две разные категории средств: предотвращение/блокирование угроз (EPP) и расширенное обнаружение и реагирование (EDR). Объединяющим элементом этих решений, в большинстве случаев, выступает антивирусный движок, который для систем класса EPP работает в режиме блокировки, а для EDR служит одним из движков, ориентированным на обнаружение сложных угроз в комплексе с другими детектирующими механизмами, такими как: IoC-сканирование, Yara-правила, песочница (поддерживают не все производители в рамках своих EDR-решений), доступ к Threat Intelligence и пр.

Отдельно стоит отметить, что в решениях класса EPP включена еще функциональность по контролю приложений и устройств, веб-контролю, оценке уязвимостей, патч-менеджменту, URL-фильтрации, шифрованию, межсетевому экранированию и пр.

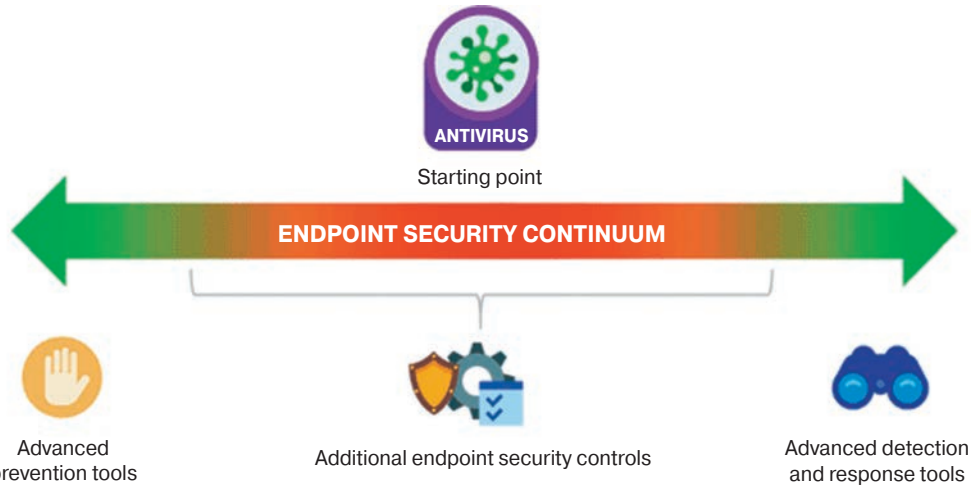

Рис. 6.6. The Endpoint Security Continuum, ESG: Redefining Next-generation Endpoint Security Solutions

Как мы видим, каждая из систем EPP и EDR сочетает в себе то, что отсутствует (или частично присутствует) в другой системе и что безусловно приводит к необходимости и важности взаимодействия этих решений. У EPP и EDR есть общая цель по противодействию угрозам, для достижения которой эти продукты используют различные подходы и функциональные возможности. Синергия использования этих решений ведет к общему более глобальному подходу защиты конечных точек.

В момент появления полнофункциональных самостоятельных систем класса EDR рынок решений по защите конечных точек был разделен на поставщиков, которые обеспечивают автоматическое предотвращение, и на тех, которые обеспечивают продвинутое обнаружение и реагирование. Хотя стоит отметить, что у пары-тройки вендоров на тот момент в портфеле уже присутствовали оба класса решений – и EPP, и EDR, но позиционировались они как совсем отдельные продукты.

Со временем произошли изменения, и большинство поставщиков начали объединять свои подходы в обеспечении как продвинутого обнаружения, так и предотвращения. Рынок решений данного класса активно развивается и формируется. Некоторые из поставщиков решений класса EPP выпустили собственные новые продукты класса EDR для получения полной картины по защите конечных устройств, другие просто доработали решения для предоставления возможности взаимодействия со сторонними поставщиками, как EPP, так и EDR-решений соответственно. Тенденция объединения решений EPP и EDR хороша для потребителей этих технологий и, вероятнее всего, продолжит развиваться в этом направлении, что должно привести к более глубокому взаимодействию этих решений. Например, к использованию единого агента на конечных точках, если это еще не реализовано в рамках одного производителя двух технологий, так и к более прозрачному взаимодействию по передаче вердиктов из EDR в EPP-решения и пр.

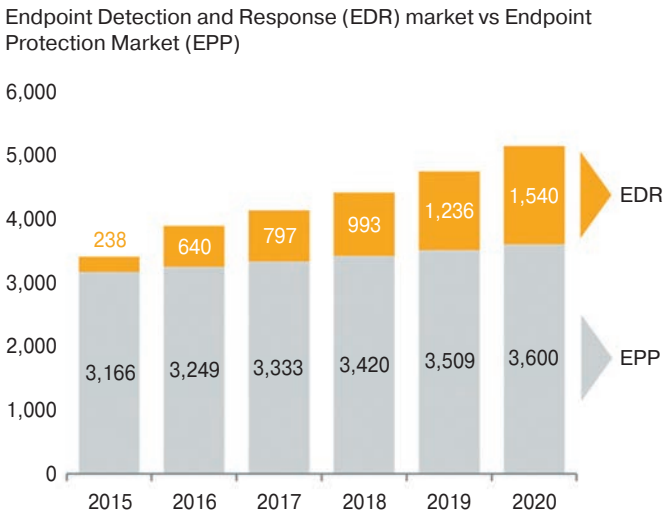

Рис. 6.7. EDR Market vs EPP Market, Gartner, CS Communications Infrastructure Team, Credit Suisse Research

Рынок все еще находится на стадии формирования. По прогнозу аналитического агентства Gartner, принимая во внимание растущую потребность в быстром и эффективном обнаружении и оперативном реагировании на передовые угрозы на конечных точках, рынок EDR-решений будет стремительно расти. В настоящее время агенты EDR-решений установлены примерно на 40 миллионах конечных точек (менее чем у 6% от общей базы конечных устройств). По оценкам Gartner, совокупные расходы организаций на решения EDR будут расти и к 2020 году составят около 1,5 млрд долларов США. Это при совокупном среднегодовом темпе роста в 45,3%, что заметно быстрее, чем прогноз совокупного среднегодового темпа роста в 2,6% для рынка решений EPP, а также чем в 7,0% для общего рынка решений по ИБ.

Аналитические агентства, вслед за формирующимися тенденциями рынка, перестраиваются в сторону формирования единых отчетов по защите конечных устройств (EPP+EDR), и уже почти каждый либо упоминает про EDR-функциональность, либо уже добавил в свои сравнительные анализы как полноценный критерий оценки.

Ведущие аналитические агентства в своих отчетах упоминают десятки производителей по защите конечных точек с включенной EDR-функциональностью. Рассмотрим кратко основные из них.

6.5. Основные платформы Endpoint Detection and Response

6.5.1. Gartner

Аналитическое агентство Gartner в ноябре 2017 года выпустило отдельный обзор рынка по EDR: Market Guide for Endpoint Detection and Response Solutions, где были детально описаны основные на тот момент направления EDR-рынка.

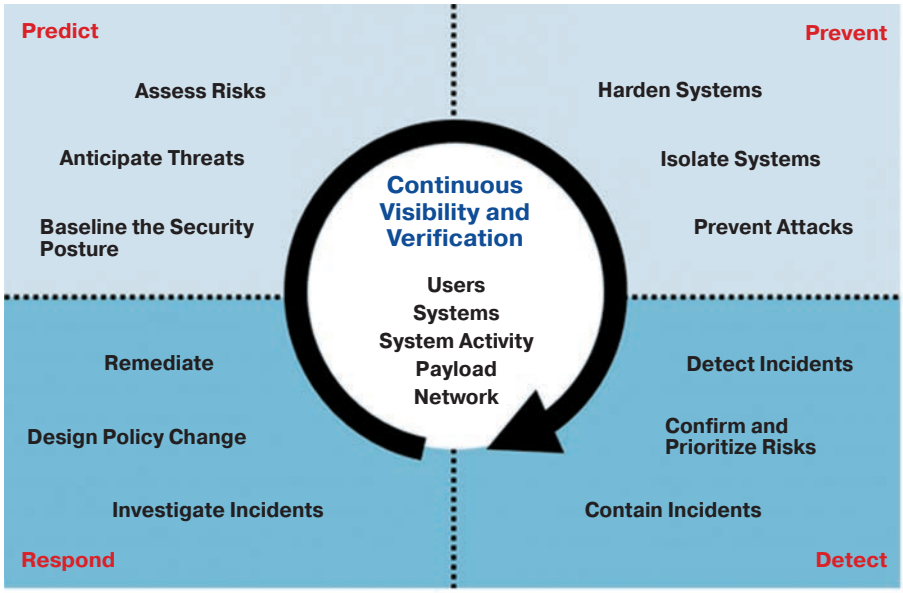

Рис. 6.8. EDR Functionality, Gartner Market Guide for Endpoint Detection and Response Solutions, 2017

В разделе Representative Vendors EDR-обзора Gartner для возможности представления масштаба рынка перечисляет следующих представителей этого рынка решений в алфавитном порядке: Carbon Black, Check Point Software Technologies, Cisco, CounterTack, CrowdStrike, Cyberbit, Cybereason, Cynet, CyTech Services, Digital Guardian, Endgame, enSilo, ESET, Fidelis Cybersecurity, FireEye, G Data Software, IBM, Kaspersky Lab, Malwarebytes, McAfee, Microsoft, OpenText (Guidance), RSA Security, Secdo, SentinelOne, Sophos, Symantec, Tanium, Trend Micro, WatchGuard, Ziften.

Также стоит отметить, что в этом обзоре Gartner начинает упоминать о важности взаимодействия решений классов EDR и EPP и, соответственно, об адаптивной стратегии: Prevent (предотвращение), Detect (обнаружение), Respond (реагирование), Predict (прогнозирование).

В январе 2018 года Gartner опубликовывает обновленную редакцию своего Магического квадранта Endpoint Protection Platforms по поставщикам решений по защите конечных устройств, где представляет полностью скорректированное определение решений класса EPP. Теперь под решениями класса EPP он понимает решения, предназначенные для контроля и блокирования угроз на конечных точках, а также продвинутого обнаружения сложных угроз и обеспечения оперативного реагирования на инциденты. Это означает, что магический квадрант Endpoint Protection Platforms за 2018 год включает решения класса EPP с включенной функциональностью EDR.

Gartner выделяет следующих производителей, находящихся в квадранте лидеров, и те компании, которые остались на один шаг от лидерства: Symantec, Sophos, Trend Micro, Kaspersky Lab, CrowdStrike.

Рис. 6.9. Gartner Magic Quadrant for Endpoint Protection Platforms, 2018

В апреле 2018 года Gartner выпустил еще один отчет касательно платформ защиты конечных точек – Critical Capabilities for Endpoint Protection Platforms, где была проведена оценка по пятибалльной шкале каждого выделенного функционального критерия. В оценке принял участие 21 производитель. Важно отметить, что Gartner в отчете относит две из девяти критически необходимых возможностей решений к EDR-технологии – это EDR Core Functionality (базовая функциональность EDR) и EDR Advanced Response (продвинутое реагирование EDR). Со всеми критериями оценки и представленными аналитическим агентством результатами в табличной форме вы можете ознакомиться в самостоятельном порядке.

6.5.2. Платформы Forrester

Международное аналитическое агентство Forrester в своем отчете The Forrester Wave™: Endpoint Security Suites за 2 квартал 2018 года частично учитывает функциональность решений класса EDR, а именно в оценке присутствует следую-

щая функциональность с учетом также функциональности систем класса EPP: automated prevention, detection, remediation, full endpoint visibility, automation, orchestration.

Лидерами по отчету Forrester на тот момент времени являлись: Bitdefender, Check Point, CrowdStrike, ESET, Sophos, Symantec, Trend Micro. К сильным игрокам на рынке Forrester причисляет следующие компании: Carbon Black, Cisco, Cylance, Kaspersky Lab, Malwarebytes, McAfee, Microsoft.

Рис. 6.10. The Forrester Wave™: Endpoint Security Suites, Q2 2018

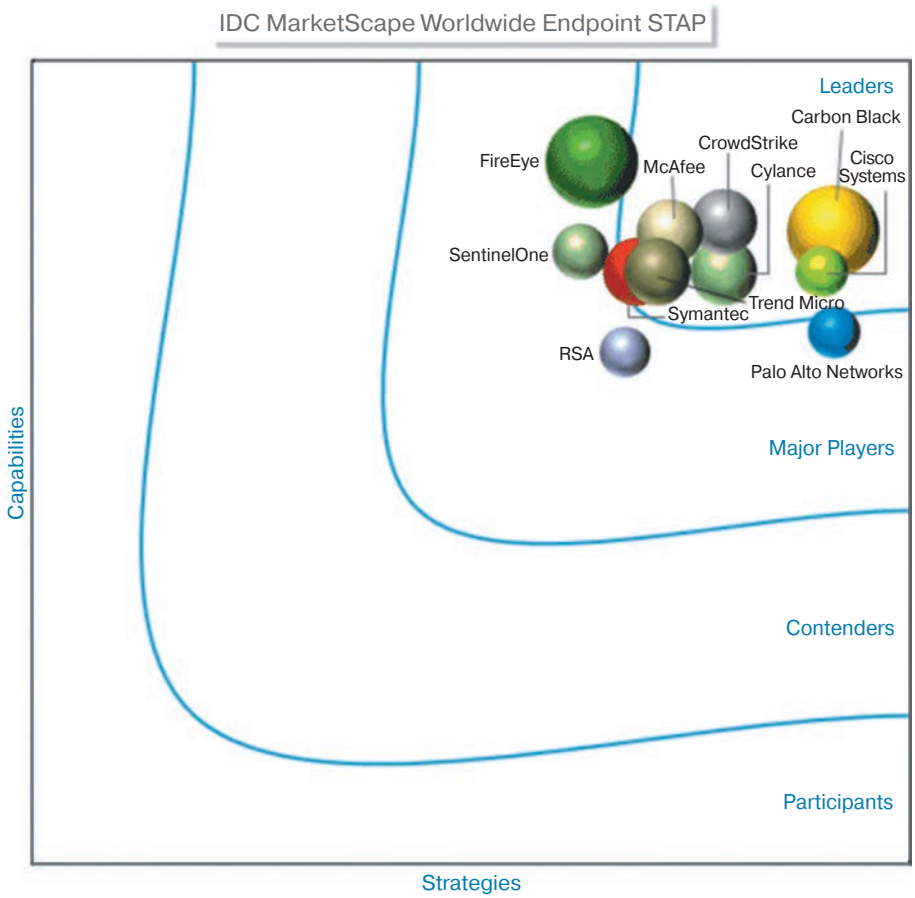

Рис. 6.11. IDC MarketScape Worldwide Endpoint Specialized Threat Analysis and Protection Vendor Assessment, 2017

IDC

Международная исследовательская и консалтинговая компания IDC в своем отчете Endpoint Specialized Threat Analysis and Protection (STAP) Vendor Assessment за 2017 г. отмечала следующих лидеров: Carbon Black, Cisco Systems, CrowdStrike, Cylance, McAfee, Symantec, Trend Micro.

6.5.3. Платформа The Radicati Group

Некоторые аналитические агентства, например The Radicati Group, сравнивали комплексные подходы к противодействию сложным угрозам, включая как сеть, так и конечные устройства, и в своем отчете Advanced Persistent Threat (APT) Protection – Market Quadrant 2018 оценивали поставщиков комплексных Anti-APT решений в соответствии со списком основных функций и возможностей, с которым вы всегда можете ознакомиться детально, изучив отчет. Отдельно выделяется критерий сравнения по предоставлению решением EDR-функциональности или возможность взаимодействия со сторонними продуктами класса EDR.

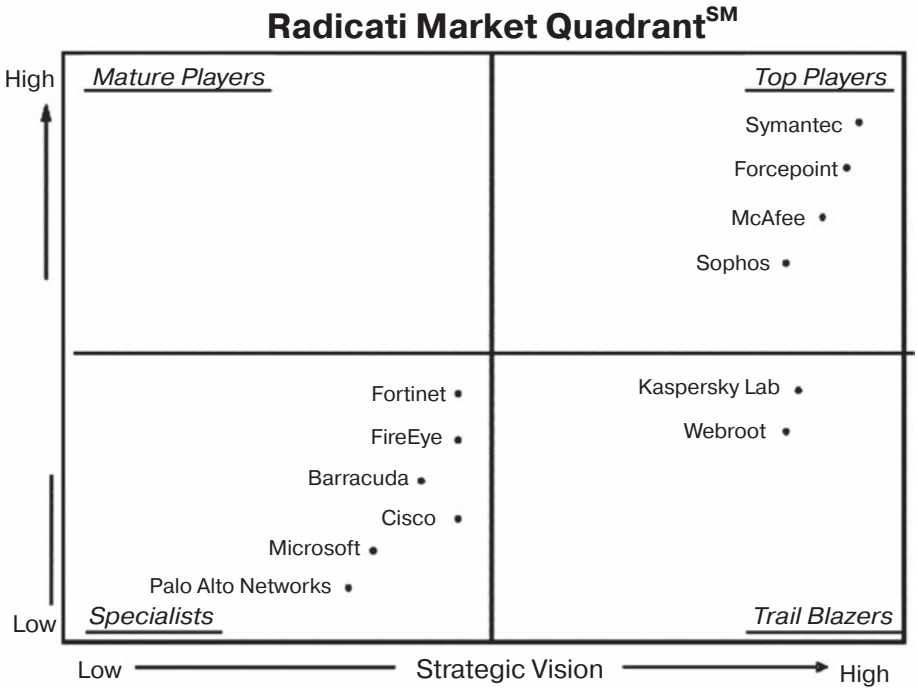

Рис. 6.12. Advanced Persistent Threat (APT) Protection – Radicati Market Quadrant, 2018

Особое внимание уделяется возможностям систем EDR по передаче собранной информации с конечных устройств в централизованную базу данных для дополнительного анализа и объединения этой информации с данными, полученными от других средств обнаружения угроз, например, на сети для получения полной картины развития возникающих угроз на всей инфраструктуре.

The Radicati Group отмечает на рынке решений по защите от APT угроз (Advanced Persistent Threat Protection) следующие компании: Barracuda Networks, Cisco, FireEye, Forcepoint, Fortinet, Kaspersky Lab, McAfee, Microsoft, Palo Alto Networks, Sophos, Symantec, Webroot.

Таким образом, в этой главе на основе обзора интернет-источников ([1] и др.) рассмотрены особенности решения задачи обеспечения кибербезопасности конечных точек инфраструктурных систем. Изощренные целевые атаки все чаще применяют сочетание распространенных угроз, детально рассмотренных нами в третьей главе, и уязвимостей нулевого дня, уникальных нестандартных схем – вообще без использования вредоносного программного обеспечения, разнообразных «бесфайловых» методов и т.п.

Присутствующие сегодня в инфраструктурах большинства организаций платформы защиты конечных точек EPP (Endpoint Protection Peatform) хорошо защищают от массовых, ранее известных угроз, но они не способны, например, определить, что поступающее предупреждение может быть составными частями более сложной и опасной атаки, которая может повлечь за собой существенный ущерб для организации.

В качестве примера эффективного решения рассмотрены платформы типа EDR (Endpoint Detection and Response), которые должны автоматически взаимосвязываться с предыдущим поколением EPP.

Рассмотрены также тенденции развития киберугроз, направленных именно на конечные точки (в том числе бесфайловых filless-атак), а также технические характеристики и особенности эксплуатации таких основных платформ EDR – решений как Gamet, Forresher, The Radicati Group.

Литература к главе 6

1. Шевченко Я. Обзор рынка Endpoint Detection and Response (EDR). URL: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-detection-and-response-edr