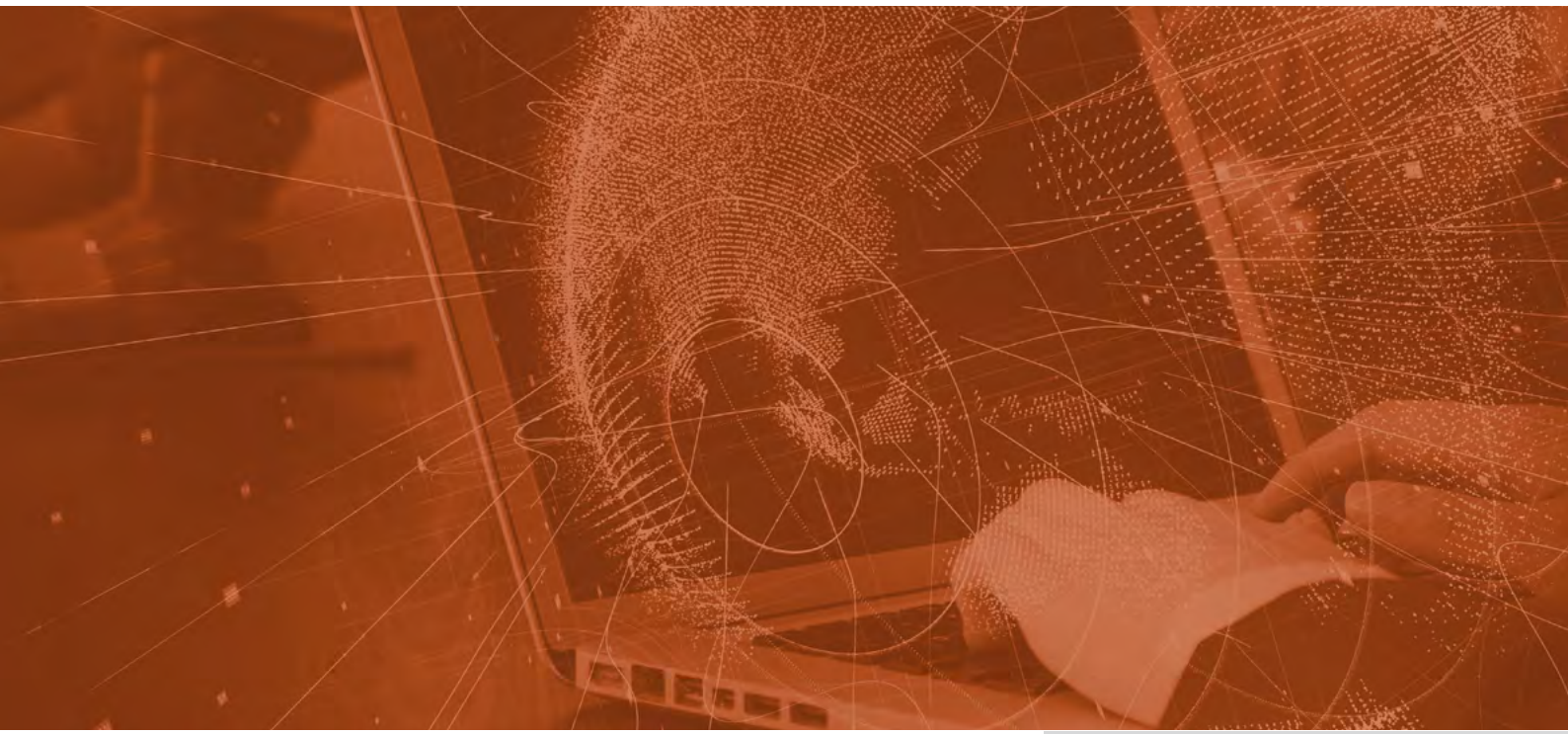
КАК ОПРЕДЕЛИТЬ, ЧТО ВЫ ПЕРЕРОСЛИ «ПЕСОЧНИЦУ» ПЕРВОГО ПОКОЛЕНИЯ



«ПЕСОЧНИЦА» ЯВЛЯЕТСЯ НЕОБХОДИМЫМ КОМПОНЕНТОМ ДЛЯ ЗАЩИТЫ ОТ ПРОДВИНУТЫХ УГРОЗ

По данным недавнего отчета, ежегодные убытки мировой экономики от действий киберпреступников превысили 450 млд долл. США. При этом было украдено более двух миллиардов личных файлов во всем мире и более 100 миллионов медицинских карт только жителей США.[1] Более 90 % нарушений безопасности[2] происходит по вине внешних злоумышленников. Пришло время пересмотреть схему работы «песочницы» в архитектуре крупных систем защиты, которые используются в современных сетях.

На сегодняшний день существует более 700 миллионов файлов вредоносных программ.[3] Одной из последних тенденций является внедрение модели «вредоносное ПО как услуга» и искусственного интеллекта (ИИ) для автоматизации высокоэффективных атак. Существует несколько основных причин, почему в качестве противодействия активно используется автоматическая система защиты с возможностями «песочницы». Ожидается, что к 2025 г. объем мирового рынка решений «песочницы» для обеспечения безопасности сети достигнет 40,48 млд долл. США.[4]

Помимо постоянного увеличения количества угроз сами сети переживают период радикального цифрового преобразования. В результате широкого распространения облачных технологий появилась потребность в интегрированных решениях безопасности, которые обмениваются данными об угрозах в распределенных сетях. Внедрение облачных технологий приводит к повышению пропускной способности по периметру сети. Поскольку компании добавляют все больше облачных сред и сред в свою расширяющуюся распределенную сеть, в таких инфраструктурах также необходимо масштабировать и систему безопасности (в том числе «песочницу») для защиты от новых уязвимостей.

На сегодняшний день существует более 700 миллионов файлов вредоносных программ.[3]

Каждый из этих факторов, а также снижение закупочных цен на устройства-песочницы и растущее желание организаций предотвратить утечку данных (а не просто ее обнаружить) — все это указывает на то, что пришло время для возрождения надежной «песочницы».

ЧЕТЫРЕ ОСНОВНЫХ ПРОБЛЕМЫ ТРАДИЦИОННЫХ «ПЕСОЧНИЦ»

К сожалению, не все «песочницы» отвечают современным требованиям, особенно решения первого поколения или традиционные «песочницы» с ограниченной производительностью и устаревшими функциями (без возможности интеграции в более широкую архитектуру безопасности или защиты от продвинутых угроз). Ниже описаны четыре основные проблемы традиционных «песочниц», которые необходимо учитывать при добавлении или обновлении «песочницы» в корпоративной сети.

ЭФФЕКТИВНОСТЬ СИСТЕМЫ БЕЗОПАСНОСТИ

Многие популярные «песочницы» недостаточно эффективны для обеспечения безопасности в эпоху, когда наиболее важно сокращать количество окон выявления и предотвращения вторжений. Чтобы минимизировать риск заражения, реакция на любое событие безопасности должна быть мгновенной. Способность продукта своевременно блокировать атаки и сообщать о заражении имеет решающее значение для обеспечения безопасности и функционирования контролируемой сети.[5]

В таком случае при оценке решения необходимо учитывать не только эффективность обнаружения угроз, но и показатели времени обнаружения, которые непосредственно влияют на рентабельность инвестиций для предприятий.[6] Чем быстрее происходит обнаружение угроз и ликвидация заражения, тем ниже затраты на восстановление.

Организациям часто приходится выбирать между способностью защитить сеть от всех видов атак и возможностью обеспечить высокую пропускную способность сети. Но для современной развивающейся архитектуры необходимы оба эти условия. Эффективность функций защиты «песочницы» следует оценивать в контексте ее производительности и наоборот.[7] Выбирайте «песочницы», имеющие рекомендации от независимых испытательных организаций (таких как NSS Labs), осуществляющих тестирование эффективности системы безопасности и времени обнаружения. Ниже перечислены дополнительные возможности, влияющие на эффективность «песочницы».

- **Интеграция.** Избегайте автономных специализированных продуктов, которые не поддерживают гибкую интеграцию в более широкую архитектуру безопасности для эффективного отслеживания и управления. Вредоносное ПО определяет присутствие виртуальной «песочницы» и избегает обнаружения, что делает технологии «песочниц» первого поколения устаревшими. Некоторые ИТ-руководители пытаются решить эту проблему путем развертывания нескольких технологий «песочницы». Но это, в свою очередь, приводит к существенному повышению сложности конфигурации, а также росту административных расходов и затрат.[8]
- **Данные об угрозах.** Кроме поддержки интеграции «песочницы» должны иметь доступ в режиме реального времени к данным об угрозах из отдела исследования угроз (а не только к информации из сторонних источников), чтобы знать о самых последних проблемах, возникающих во всем мире. «Песочница» должна выступать в качестве центра обнаружения угроз «нулевого дня», обмениваясь последней информацией с другими средствами защиты и компонентами архитектуры для обеспечения скоординированного и автоматизированного реагирования на атаки. Когда различные решения, интегрированные в архитектуру безопасности, обмениваются между собой данными, вместе они обеспечивают гораздо более высокую эффективность, чем в сумме по отдельности.[9]
- **Обнаружение и предотвращение.** Обнаружение вторжений вредоносного ПО должно быть быстрым и точным, чтобы администраторы смогли сдержать распространение заражения и минимизировать воздействие на сеть.[10] Хотя все «песочницы» имеют функции обнаружения угроз, они также должны предотвращать атаки прежде, чем вредоносное ПО проникнет в сеть и получит доступ к конфиденциальным данным. Превентивная способность «песочницы» быстро блокировать атаки и сообщать о потенциальных угрозах является крайне важной. Организациям следует выбирать решение, поддерживающее функции обнаружения и предотвращения вторжений (иногда это называется защитой от продвинутых угроз).
- **Собственные технологии.** Избегайте «песочниц», которые разработаны на базе общих технологий, лицензированных OEM-производителями, для разных поставщиков. В случае истечения срока действия договора или, если лицензиар медленно обновляет исходный код, организация может получить неэффективный продукт практически без возможности решить эту проблему. Наиболее эффективные «песочницы» созданы на основе оригинальных технологий, разработанных самим производителем. Такие компании обычно следят, чтобы их решения всегда были в актуальном состоянии, не имели уязвимостей и поддерживали самые новые и лучшие функции для текущего состояния картины угроз.

АДМИНИСТРАТИВНЫЕ РАСХОДЫ

Во всем мире отделы ИТ-безопасности сталкиваются с проблемой жесткого ограничения бюджета и нехватки квалифицированных специалистов. Например, 45 % организаций жалуются на нехватку специалистов по информационной безопасности.[11] На отделы безопасности ложится огромная нагрузка и им необходимо повышать производительность везде, где это возможно. Администрирование многих устаревших «песочниц» приходится осуществлять вручную, что еще больше увеличивает нагрузку на сотрудников. Ниже перечислены ключевые факторы, которые необходимо учитывать.

- **Упрощение управления системой безопасности.** Выбирайте «песочницы», которые обмениваются данными об угрозах «нулевого дня» со всеми внутренними средствами управления безопасностью с целью автоматического применения надлежащих мер защиты сети. Помимо всего прочего, это помогает устранить ручные процессы и снизить нагрузку, связанную с управлением.

На отделы безопасности ложится огромная нагрузка и им необходимо повышать производительность.

45 % организаций испытывают нехватку специалистов по информационной безопасности.[11]

- **Развертывание и форм-факторы.** Простота интеграции является вторым по важности критерием для американских предприятий во время принятия решений о покупке продуктов безопасности (после стоимости).[12] Решения с форм-факторами для работы только в локальном режиме могут ограничивать варианты использования «песочницы». Также решения, использующие только физические подключения (такие как компоненты сети TAP) значительно повышают время и стоимость развертывания «песочницы» в организации.

МАСШТАБИРУЕМОСТЬ

При использовании многих традиционных «песочниц» возникают проблемы с масштабированием, касающиеся поддержки растущего потока трафика или изменений инфраструктуры в рамках проектов по цифровой трансформации.(например, расширение в различные облачные среды). В условиях отсутствия последних технических возможностей возникает необходимость в приобретении дополнительных устройств, что приводит к повышению расходов и сложности процесса масштабирования «песочницы». Также распространенными проблемами, возникающими при масштабировании, являются нехватка производительности, ограничения лицензирования и физические ограничения развертывания.

- **Лицензирование.** Помимо физических проблем с устаревшими разъемами и ограниченными форм-факторами, чрезмерно сложные и дорогие модели лицензирования могут ограничивать возможности экономичного развертывания решения по мере расширения среды.
- **Количество узлов в кластере.** Выбирайте «песочницу», которая поддерживает большое количество узлов в кластере, чтобы быть готовыми к росту сети, увеличению потока трафика и повышению требований к системе безопасности в будущем.

СТОИМОСТЬ

Процесс внедрения песочницы может быть очень сложным, при этом множество факторов влияют на совокупную стоимость развертывания, технического обслуживания и содержания.[13] Для многих «песочниц» необходимо использовать несколько устройств и/или подписок, что приводит к повышению совокупной стоимости владения (TCO). Ниже перечислены основные критерии, требующие рассмотрения.

- **Поверхность атаки.** Независимо от того, хотите ли вы оценить существующее решение, обновить его или добавить «песочницу» в первый раз, рассматривайте решение в комплексе и учитывайте все связанные с этим расходы. Ответьте на следующие вопросы. Охватывает ли «песочница» всю поверхность атаки (сеть, конечные точки, Интернет, электронную почту и облако) без дополнительных лицензий и расходов? Поддерживает ли она такие важные функции, как проверка трафика SSL и TLS?
- **Стоимость каждого защищенного Мбит/с.** Для замены «песочницы» организациям следует выбирать решения, которые помогают сократить стоимость каждого защищенного Мбит/с (на основе тестирования, проведенного независимой организаций, такой как NSS Labs) и устранить дополнительные расходы на подписку.

ВЫХОД ЗА ПРЕДЕЛЫ ТРАДИЦИОННОЙ «ПЕСОЧНИЦЫ» ПЕРВОГО ПОКОЛЕНИЯ

«Песочницы» предыдущего поколения могут значительно отставать от скорости и сложности современных угроз или не соответствовать изменениям сетевых инфраструктур, вызванным развитием цифровых технологий. Но несмотря на это, «песочница» по-прежнему остается необходимым компонентом интегрированной архитектуры безопасности.

[1] The Hiscox Cyber Readiness Report 2017, Hiscox Insurance Company Inc., редакция от 21 марта 2018 г.
[2] 2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter, Verizon, 26 июля 2017 г.
[3] Malware, AV-TEST, 9 апреля 2018 г.
[4] Network Security Sandbox Market Analysis By Solution, By Services (Professional Consulting,Maintenance, Subscription), By Application, By Region, And Segment Forecasts, 2014 – 2025, Grand View Research, ноябрь 2017 г.
[5] Breach Prevention Systems Test Report, NSS Labs, 13 декабря 2017 г.
[6] NSS Labs Announces 2017 Breach Detection Systems Group Test Results, NSS Labs, 19 октября 2017 г.
[7] Breach Prevention Systems Report, NSS Labs, 13 декабря 2017 г.
[8] Ник Исмаил (Nick Ismail), Is your sandbox strategy keeping you safe? Information Age, 6 июля 2017 г.
[9] Джейсон Паппалексис (Jason Pappalexis), Breach Prevention Systems and the Importance of Interoperability, NSS Labs, 6 февраля 2018 г.
[10] Уильям Дин Фримен (William Dean Freeman) и Джессика Уильямс (Jessica Williams), Breach Prevention Systems Test Report, NSS Labs, 13 декабря 2017 г.
[11] Джон Олтсик (Jon Oltsik), Cybersecurity skills shortage creating recruitment chaos, CSO, 28 ноября 2017 г.
[12] Джейсон Паппалексис (Jason Pappalexis), Breach Prevention Systems and the Importance of Interoperability, NSS Labs, 6 февраля 2018 г.
[13] Breach Prevention Systems Test Report, NSS Labs, 13 декабря 2017 г.

FORTINET В РОССИИ
Пресненская набережная 10,
блок С
123317 Москва
Тел: +7 495 937 80 50
Эл. адрес: russia@fortinet.com

ГЛАВНЫЙ ОФИС
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
США
Тел.: +1 408 235 7700
www.fortinet.com/sales

ОТДЕЛ ПРОДАЖ В ЕВВА
905 rue Albert Einstein
06560 Valbonne
Франция
Тел.: +33 4 8987 0500

ОТДЕЛ ПРОДАЖ В АТР
300 Beach Road 20-01
The Concourse
Сингапур 199555
Тел.: +65 6513 3730

ЛАТИНСКАЯ АМЕРИКА ГЛАВНЫЙ ОФИС
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Тел.: +1 954 368 9990

декабря 3, 2018 11:14 AM