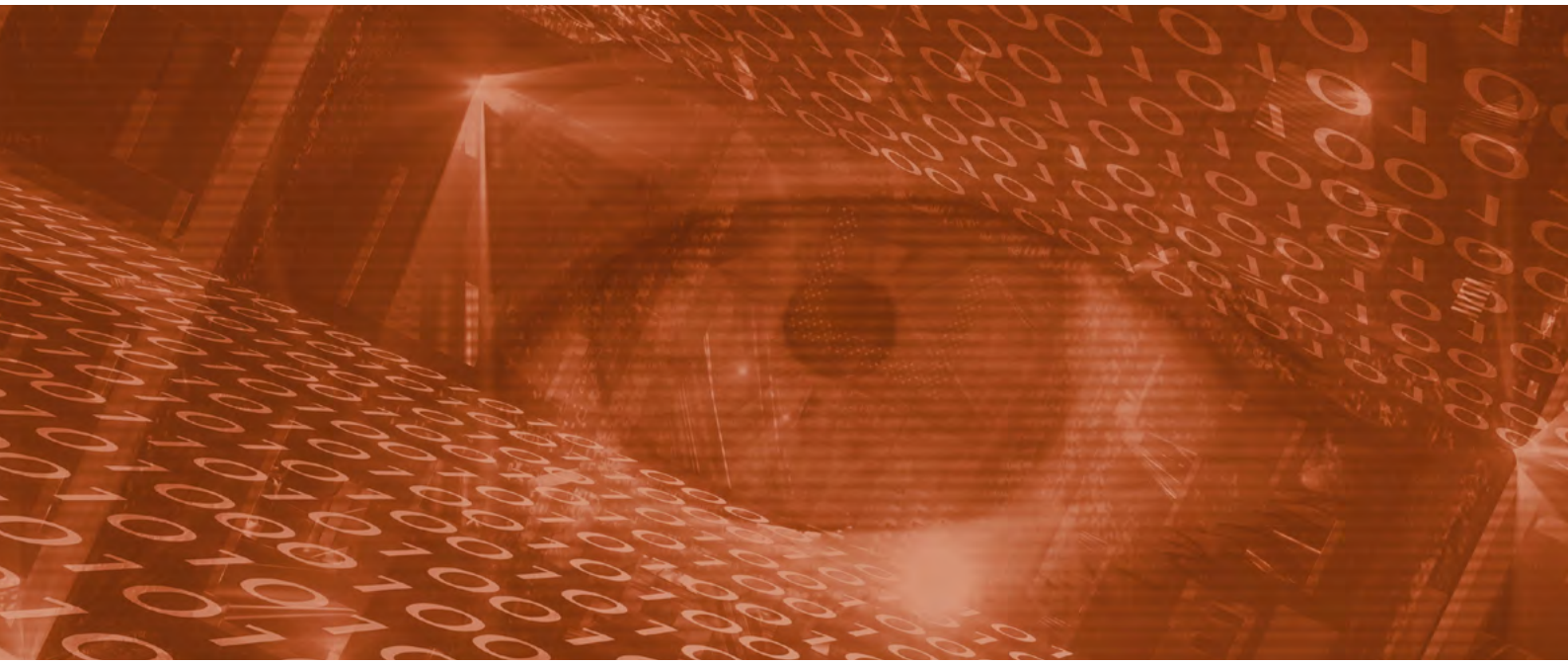
ОБЗОР ТРЕБОВАНИЙ К «ПЕСОЧНИЦЕ» СЛЕДУЮЩЕГО ПОКОЛЕНИЯ, КАК ИСТРУМЕНТУ ДЛЯ ЗАЩИТЫ ОТ ПРОДВИНУТЫХ УГРОЗ



АННОТАЦИЯ

Поскольку сетевые инфраструктуры расширяются, включая в себя новые сервисы и технологии для повышения гибкости бизнеса, системы безопасности также должны развиваться, чтобы прогнозировать постоянно растущую уязвимость перед новыми еще неизвестными угрозами. «Песочница» является важной частью архитектуры системы безопасности, обеспечивающей выявление и предотвращение угроз до того, как они смогут повлиять на коммерческую деятельность. Но многие «песочницы», старые и новые, не отвечают требованиям современных сетей. При добавлении или замене «песочницы» организациям следует обратить внимание на решения, которые предлагают несколько конкретных функций и возможностей следующего поколения.

НА ЧТО СЛЕДУЕТ ОБРАТИТЬ ВНИМАНИЕ ПРИ ВЫБОРЕ «ПЕСОЧНИЦЫ»

На фоне цифровой трансформации сетевых инфраструктур, быстро меняющихся угроз и новых требований бизнеса технологии «песочницы» должны постоянно развиваться и предлагать возможности следующего поколения. Но на рынке все еще много устаревших решений, которые не идентифицируют себя в качестве «первого поколения», а также решений, функциональности которых недостаточно для противостояния современным угрозам. Покупатели должны понимать свои требования к «песочнице», чтобы основательно дополнить имеющуюся и будущую архитектуру безопасности.

Организациям, которые оценивают имеющуюся у них «песочницу», необходимо убедиться в наличии следующих основных атрибутов «песочницы» следующего поколения, которые действительно помогают противостоять продвинутым угрозам.

1. Интеграция и автоматизация

Многие технологии «песочницы» располагаются в собственных средах в виде изолированных специализированных устройств. Это означает, что они не могут обмениваться данными об угрозах с другими компонентами системы безопасности в организации, а также получать и использовать подобную информацию.

Это проблематично, поскольку сложные угрозы нацелены на широкую поверхность атаки при попытке проникнуть в сеть организации. Либо они могут быть настолько новыми, что для них просто еще нет результатов независимых оценочных испытаний. Чтобы противостоять подобным атакам, нужна «песочница», взаимодействующая с более масштабной архитектурой системы безопасности. В частности, интеграция предоставляет возможность системе обмениваться данными об угрозах «нулевого дня» со всеми внутренними средствами управления безопасностью, которые автоматически применяют надлежащие меры защиты. Это помогает устранить ручные процессы, сократить время реагирования и снизить нагрузку, связанную с управлением, — особенно для организаций, где стоит проблема нехватки квалифицированных специалистов по безопасности.

Бесшовная интеграция в автоматическом режиме упрощает управление системой безопасности, обеспечивает возможность комплексного отслеживания, а также быстрое и простое развертывание «песочницы». Не используйте устройства, которые необходимо подключать через компоненты сети TAP, поскольку это удлиняет циклы развертывания и требует вмешательства при каждом изменении сетевых портов или виртуальных локальных сетей (VLAN).

2. Обнаружение и предотвращение

Многие «песочницы» предлагают только возможности обнаружения угроз. Но ключевым условием для минимизации воздействия угроз на корпоративную сеть является защита от продвинутых угроз. По данным независимой исследовательской организации NSS Labs, когда дело доходит до систем предотвращения вторжений, процессы обнаружения угроз и предотвращения вторжений тесно связаны между собой. В последнем отчете NSS Labs, посвященном системам предотвращения вторжений, говорится: «Способность решения блокировать атаки и своевременно сообщать о заражении является важным условием для обеспечения безопасности и функционирования контролируемой сети. О заражении и проникновении вредоносного ПО необходимо сообщать быстро и точно, чтобы администраторы могли сдержать распространение заражения и минимизировать влияние на сеть».[1]

Чтобы убедиться, что оцениваемое решение «песочницы» действительно обеспечивает обнаружение и предотвращение вторжений, необходимо проверить наличие независимой сертификации и рекомендаций от внешних испытательных организаций. Области оценки должны включать совокупную стоимость владения (TCO), время обнаружения, возможности обхода и эффективность защиты как при обнаружении вторжений, так и при их предотвращении. Избегайте решений, для которых имеются предостережения или другие оценки, не рекомендующие их использование, а также решений, для которых не проводились никакие тестирования систем обнаружения и предотвращения вторжений.

3. Проверка SSL/TLS

Чтобы соответствовать нормативным требованиям, многие предприятия должны защищать определенные типы конфиденциальных данных с помощью шифрования уровня защищенных сокетов (SSL) или безопасности уровня транспорта (TLS). В настоящее время доля зашифрованного содержимого составляет 60 % от всего объема сетевого трафика и каждый год эта цифра продолжает расти.[2] Но киберпреступники также могут использовать шифрование, чтобы скрыть вредоносное ПО и программы-вымогатели от традиционных решений обеспечения корпоративной информационной безопасности.

В этой ситуации со многими «песочницами», доступными на рынке, возникают проблемы. Поскольку в большинстве случаев они зависят от дополнительных сторонних устройств для проверки зашифрованных данных. В таком случае руководителям отдела безопасности и сетевым администраторам необходимо найти такую «песочницу», которая будет иметь доступ к надежным инструментам проверки зашифрованных данных посредством интеграции с существующими средствами управления безопасностью, такими как межсетевые экраны следующего поколения.

4. Масштабируемость

Ожидаемый рост инфраструктуры — это еще один аспект оценки, насколько «песочница» подойдет для растущей архитектуры системы безопасности. Идеальное решение должно поддерживать высокую пропускную способность и масштабируемость для потенциального или запланированного расширения бизнеса в будущем.

Что касается масштабируемости, то большое количество узлов в кластере помогает поддерживать актуальность «песочницы» в соответствии с изменениями, которые со временем могут привести к повышению требований к безопасности. Например, сейчас предприятия стремятся расширять возможности песочницы для защиты облака, чтобы использовать преимущества гибкости облачных технологий. Высокий уровень масштабируемости и доступности решения является очень важным требованием, поскольку в эпоху цифровых преобразований корпоративные сети постоянно расширяются.

5. Оригинальные технологии

Многие поставщики «песочниц» используют по лицензии технологии крупных производителей оригинального оборудования (OEM), применяемые в их продуктах. Поскольку эти компании не производят все предоставляемое аппаратное и/или программное обеспечение и не владеют им, они остаются зависимы от лицензиаров в вопросах, касающихся выпуска обновлений и исправлений и обеспечения эффективности продукта. В случае истечения срока действия лицензии на решение стороннего поставщика или ее изменения до окончания срока эксплуатации вашего продукта, инвестиции, вложенные в эту «песочницу», могут не окупиться. Еще хуже, когда «песочница» создана на базе технологий с открытым кодом, который также доступен создателям вредоносного ПО.

Выбирайте поставщиков, которые создают решения на базе собственных оригинальных технологий. Руководителям отдела безопасности и сетевым администраторам необходимо, чтобы решения всегда были в актуальном состоянии, не имели уязвимостей и поддерживали самые новые и лучшие функции для противостояния текущим угрозам. Если поставщик использует собственные решения, это означает, что вам будет обеспечено постоянное улучшение продуктов, получение компетентной поддержки, доступ к учебным ресурсам и (самое важное) своевременное исправление ошибок в системе безопасности.

6. Форм-фактор

Выбирайте «песочницу», которая поставляется в нескольких форм-факторах. Поскольку виртуализация и внедрение облачных технологий используются все активнее, для большинства организаций локальной «песочницы» будет недостаточно. В эпоху цифровых преобразований предприятиям необходима гибкость для использования «песочницы» в разных форм-факторах — в виде локального устройства, виртуальной машины и/или в облаке.

Организациям малого и среднего бизнеса с инфраструктурой, размещенной в облаке, локальная «песочница» может быть не нужна. Кроме того, наличие нескольких форм-факторов гарантирует беспроблемный переход из одной среды в другую. Например, предприятие может планировать поэтапный переход в облако в течение трех лет в рамках цифрового преобразования для перемещения внутренних и внешних служб и приложений из центра обработки данных в облако. При этом на сегодняшний день им необходимо обеспечивать безопасность ресурсов в текущем центре обработки данных. Локальное решение может защищать существующую инфраструктуру, поддерживая плавный переход в облако по мере необходимости и обеспечивая постоянную защиту, настройку и управление лицензиями.

7. Снижение совокупной стоимости владения

Современная песочница должна быть универсальным решением, которое взаимодействует с более масштабной архитектурой системы безопасности. Выбирайте одно устройство с одной подпиской, поддерживающее интеграцию с другими компонентами архитектуры безопасности, чтобы охватить всю поверхность атаки (сеть, конечные точки, Интернет, электронную почту и облако) без дополнительных лицензий и расходов. Не используйте «песочницы», требующие несколько устройств, лицензий и/или подписок на получение данных об угрозах.

Сравните соотношение цены и производительности (стоимость каждого защищенного Мбит/с) решений, рассчитанное в рамках независимого тестирования. Необходимо учитывать не только затраты на приобретение «песочницы» и лицензии, но и эксплуатационные расходы, такие как время, потраченное сотрудниками на управление решением, обслуживание, регистрация данных и создание отчетов.

ПОИСК «ПЕСОЧНИЦЫ» СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

На рынке представлено много устаревших продуктов и решений с ограниченной функциональностью, которые не следует использовать. Но знание характеристик, на которые необходимо обращать внимание, поможет избежать ошибок и найти лучшую «песочницу» для защиты от вредоносного ПО и других угроз, связанных с сетевым трафиком.

«Песочница», удовлетворяющая требованиям современных сетей, не всегда может называться решением следующего поколения, но она всегда будет отвечать следующим критериям:

- Защита от продвинутых угроз
- Обнаружение новых угроз на основе исследования потенциальных угроз/данных об угрозах
- Независимая сертификация и рекомендации по результатам тестирования
- Поддержка проверки зашифрованного трафика (SSL/TLS)
- Большое количество узлов в кластере для обеспечения масштабируемости
- Оригинальные технологии, разработанные поставщиком
- Несколько вариантов форм-фактора
- Одно устройство, одна лицензия, одна подписка

[1] Уильям Дин Фримен (William Dean Freeman) и Джессика Уильямс (Jessica Williams), Breach Prevention Systems Test Report: Fortinet Advanced Threat Protection, NSS Labs, 13 декабря 2017 г.

[2] См., например, Дж. Майкл Батлер (J. Michael Butler), SANS Institute InfoSec Reading Room: Finding Hidden Threats by Decrypting SSL, ноябрь 2013 г.; Джонни Константас (Johnnie Konstantas), SSL Encryption: Keep Your Head in the Game, SecurityWeek, 15 марта 2016 г.

декабря 3, 2018 1:00 PM