

RSA® ARCHER® CONTINUOUS MONITORING

Сценарий использования для решений в публичном секторе

Сложности

Организации редко проводят оценку средств управления безопасностью. При этом они выполняют ее, используя инструменты от различных поставщиков с проприетарными форматами и ограниченными возможностями по обмену данными. А после этого персонал не справляется с обработкой данных и не может определить приоритеты по устранению проблем с применением всех доступных контекстуальных данных. Непрерывный мониторинг (CM) представляет собой комбинацию оценок, выполняемых вручную и автоматически. Каждый поставщик, который производит инструменты автоматического сканирования или обнаружения, представляет свой продукт как «решение для непрерывного мониторинга». Но они не предлагают средства для ручных оценок и часто выполняют проверку на дефекты только одного типа (уязвимость или ошибки в конфигурации), тогда как рекомендации по непрерывному мониторингу от Института стандартов и технологий США (NIST) и Министерства национальной безопасности США включают множество типов дефектов. Обновления закона Federal Information Security Management Act (FISMA) и последние рекомендации Учреждения по управлению и бюджету (OMB) вынуждают организации развивать непрерывный мониторинг, но при этом они не имеют достаточно данных для эффективной реализации.

До этого момента отсутствие непрерывного мониторинга среди федеральных учреждений означало наличие дефектов и уязвимостей. Это также усложняет общий обмен данными или создание комплексного представления рисков вследствие разрозненности инструментов и наличия неполных и устаревших результатов оценок. Кроме того, не хватает специалистов для выполнения всех оценок и устранения всех найденных проблем. Отсутствие контекста и визуализации означает, что самые критические дефекты не устраняются в первую очередь. Например, следует ли сначала устранить критическую проблему в системе средней важности или проблему средней важности в критической системе? Большинство организаций не имеют нужных средств анализа и метрик для классификации дефектов, особенно с учетом критичности информационных систем.

Обзор

RSA® Archer® Continuous Monitoring выполняет роль концентратора для различных инструментов сканирования и обнаружения, что позволяет организации создать агрегированное представление рисков на любом уровне предприятия. Решение позволяет отслеживать и оценивать отдельные дефекты на самом низком уровне. Затем они агрегируются на каждом уровне иерархии — от отдельных устройств до уровня подразделений. Таким путем можно классифицировать риск на любом уровне и определить объем относительного риска. Это позволяет сосредоточить ограниченные ресурсы на устранении дефектов, что намного эффективнее.

С RSA Archer Continuous Monitoring вы можете быстрее и точнее реагировать на возникающие риски. Ваш персонал сможет действовать таким образом, чтобы как можно быстрее и максимально сократить риски. При использовании с RSA Archer Assessment and Authorization решение может улучшить выполнение требований закона FISMA и OMB путем проверки выполнения информационными системами авторизационных соглашений (разрешений на эксплуатацию — ATO) и допустимого уровня риска. Это улучшит безопасность среды, позволит лучше понимать ее и принимать более взвешенные решения по рискам.

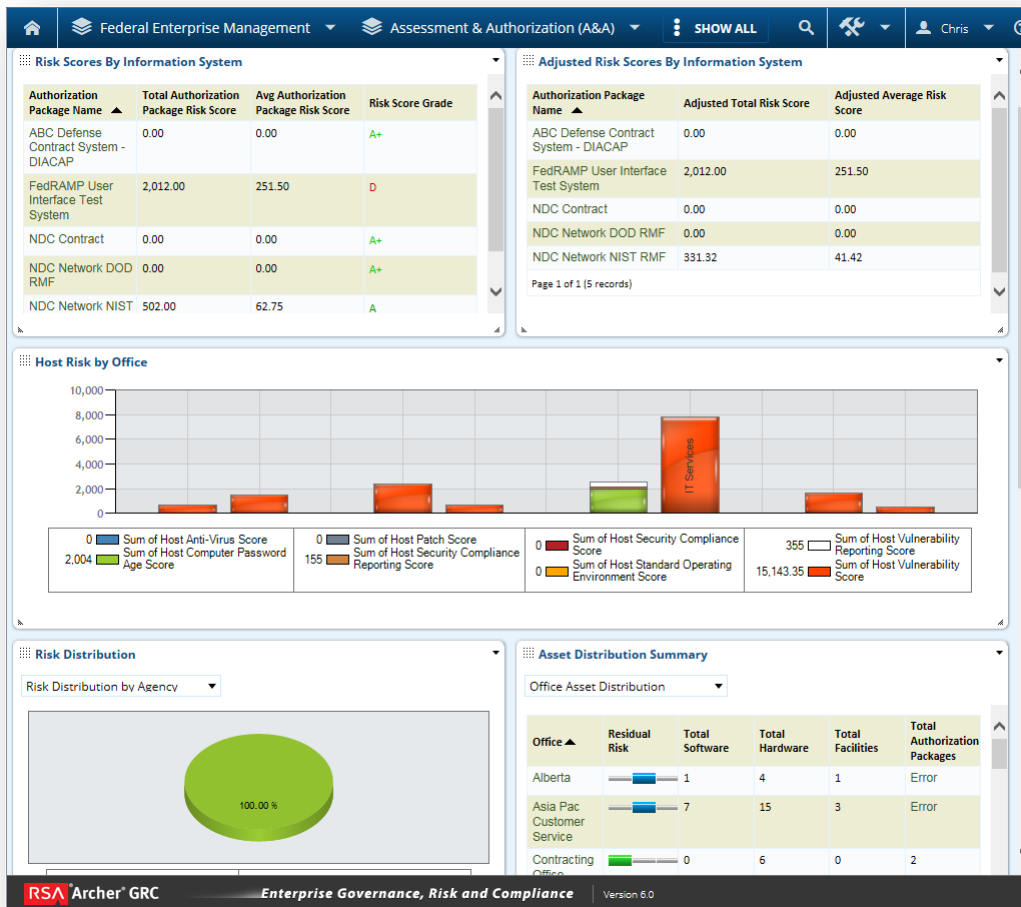
Основные характеристики

- Актуальные и точные реестры оборудования и ПО.
- Актуальные библиотеки дефектов.
- Интеграция средств сканирования и обнаружения в общую среду в общем формате.
- Алгоритмы оценки и классификации для каждого дефекта, устройства и уровня в организационной иерархии.
- Отслеживание и устранение дефектов.

Ключевые преимущества

RSA Archer Continuous Monitoring предоставляет следующие преимущества.

- Сокращенное время уязвимости.
- Общее сокращение рисков.
- Улучшенная визуализация и принятие более взвешенных решений.
- Актуальные данные по рискам.
- Дополнительная уверенность благодаря актуальным данным.



Дополнительные сведения

Чтобы получить более подробную информацию о том, как продукты, услуги и решения EMC помогают решать сложности бизнеса и ИТ, свяжитесь с локальным представителем или авторизованным реселлером либо посетите наш веб-сайт по адресу www.rsa.com. Если у вас, как у заказчика RSA Archer, имеются вопросы, или вам необходима дополнительная информация о лицензировании, напишите письмо в подразделение RSA Archer по адресу электронной почты archersupport@rsa.com или позвоните по номеру 1-888-539-EGRC.