RED Check

RedCheck – система контроля защищенности и соответствия стандартам, предоставляющая широкий круг возможностей по управлению информационной безопасностью для предприятий любого масштаба.

Система предназначена для получения данных о параметрах ИТ-инфраструктуры и их значениях, влияющих на защищенность объектов информатизации, а также для поддержки принятия решений по устранению выявленных уязвимостей и созданию эффективных конфигураций безопасности контролируемых систем.

Сканер разработан с учетом потребностей отечественных компаний в области информационной безопасности и требований российских Регуляторов. RedCheck позволяет решать широкий спектр задач: от поиска уязвимостей до оценки соответствия отечественным и международным стандартам безопасности, а также реализовывать ряд мер защиты, обязательных для информационных систем персональных данных (ИСПДн), государственных информационных систем (ГИС), автоматизированных систем управления производственными и технологическими процессами (АСУ ТП), значимых объектов критической информационной инфраструктуры (ЗО КИИ) и автоматизированных систем, обрабатывающих конфиденциальную информацию.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ:

АУДИТ УЯЗВИМОСТЕЙ

Проведение проверок на предмет наличия уязвимостей узла, обусловленных ошибками кода, которые могут быть использованы внешним или внутренним нарушителем.

АУДИТ И УСТАНОВКА ОБНОВЛЕНИЙ

Поиск и установка недостающих обновлений безопасности на узлах сети, в том числе при помощи Microsoft WSUS. Объектами аудита являются все актуальные клиентские и серверные операционные системы, а также широкий перечень общесистемного и прикладного ПО.

АУДИТ КОНФИГУРАЦИЙ

Контроль конфигураций и оценка соответствия политикам безопасности.

АУДИТ СУБД

Проведение аудита СУБД на предмет уязвимостей, критичных неустановленных обновлений, а также проведение контроля безопасности конфигурации как самой СУБД, так и её среды функционирования.

АУДИТ СЕРВЕРОВ ПРИЛОЖЕНИЙ

Отдельное направление аудита для проверки специальных конфигураций для серверов приложений, Web-серверов и их компонентов. RedCheck позволяет выявлять потенциально небезопасные настройки параметров безопасности как на уровне операционной системы и сервера приложений, так и на уровне отдельного web-сайта или ресурса.

АУДИТ ПЛАТФОРМ ВИРТУАЛИЗАЦИИ

Детальный аудит платформ виртуализации (инвентаризация, уязвимости, обновления, конфигурации, контроль целостности) для Hyper-V и VMware.

ИНВЕНТАРИЗАЦИЯ

Реализованный в системе функционал инвентаризации обеспечивает сбор информации о составе технических средств и установленном (запущенном) программном обеспечении на узле сети. Для функции «Инвентаризация» предусмотрен механизм контроля, который позволяет зафиксировать состояние аппаратной и/или программной среды узла и с заданной периодичностью осуществлять контроль ее изменения.

ФИКСАЦИЯ И КОНТРОЛЬ

Контроль целостности папок, файлов и веток реестра (для Windows) узлов сети. Выбор объектов фиксации осуществляется из произвольного каталога или по маске (расширению) файла. При формировании заданий можно создавать исключение неконтролируемых файлов из фиксируемых каталогов.

СКАНИРОВАНИЕ ПОРТОВ

Сканирование портов позволяет определить доступную об исследуемых узлах сети информацию, такую как: открытые порты, протоколы работы портов, сетевые сервисы и т.д. Получение информации происходит при минимальном уровне привилегий.

ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ АУДИТА

Детализированные и интегральные отчеты по каждому направлению аудита.

СОВМЕСТИМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

СИСТЕМА ОБЕСПЕЧИВАЕТ АНАЛИЗ ЗАЩИЩЕННОСТИ СЛЕДУЮЩИХ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ:

- клиентские операционные системы Microsoft Windows XP/ Vista/7/8/8.1/10;
- серверные операционные системы Microsoft Windows Server 2003/2008/2008R2/2012/2012R2/2016
- операционные системы Linux: CentOS, Debian, Oracle Linux, openSUSE, Red Hat, SUSE, Ubuntu, Cisco iOS, Astra Linux, ALT Linux;
- платформы виртуализации VMware, Microsoft Hyper-V;
- СУБД Microsoft SQL Server 2005-2016, Oracle Database Server 11/12, PostgreSQL, IBM DB2;
- сетевое оборудование Cisco, Huawei, Булат, Check Point;
- офисные пакеты Microsoft Office 2003-2016, LibreOffice, Adobe
- веб-сервера и приложения Apache, nginx, IIS, Apache Tomcat, .NET Framework;
- а также более 700 различный приложений.

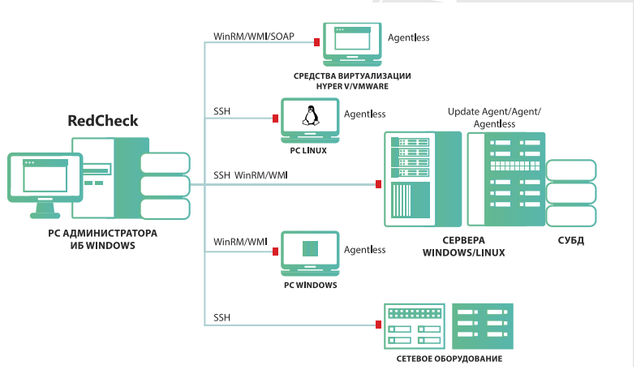
АРХИТЕКТУРА

Гибкая архитектура и система лицензирования позволяет разворачивать RedCheck как в локальной сети или отдельном узле, так и выстраивать иерархически подчиненные структуры, позволяющие получать полную картину состояния защищенности всей системы или отдельных ее сегментов. RedCheck не имеет ограничений по масштабированию.

ВОЗМОЖНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ:

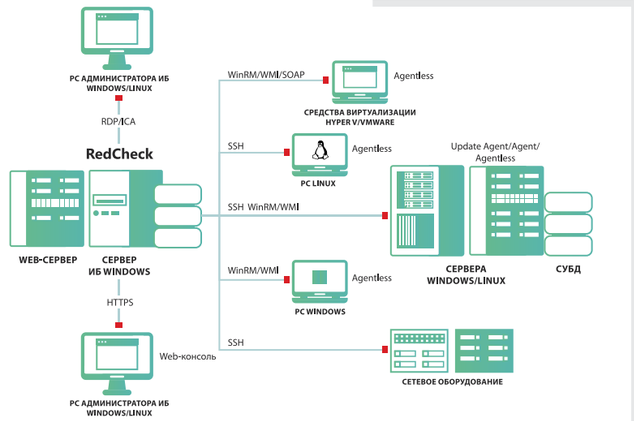
Контроль защищенности малых и средних сетей (АРМ администратора безопасности)

Для контроля малых и средних сетей (до 200 узлов) RedCheck может быть непосредственно развернут на АРМ администратора (администратора безопасности) без существенной потери производительности компьютера. Также RedCheck может быть установлен на ноутбук для проведения выездных проверок (аудита).



Контроль защищенности территориально удаленной сети (Установка на выделенный сервер)

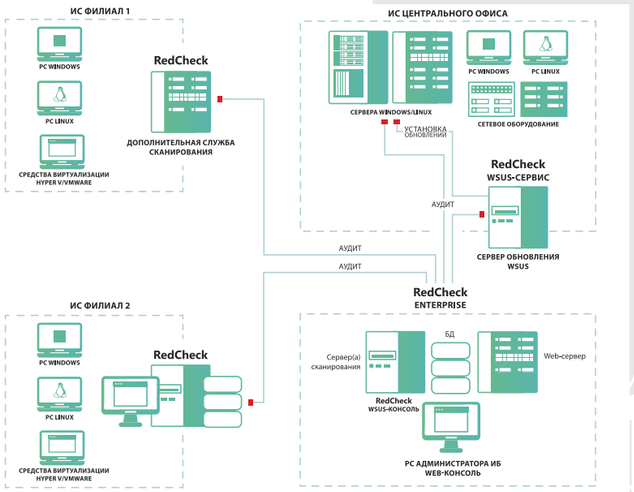
Наличие в RedCheck разнообразных транспортов и протоколов управления позволяет осуществлять удаленное сканирование сети любого масштаба по всем направлениям аудита без существенной нагрузки на каналы связи. Для повышения скорости сканирования Windows-систем и снижения сетевого трафика рекомендуется использование агента программы RedCheck Agent или Remote Engine (WinRM).



Контроль (анализ) защищенности крупных сетей и сетей с филиальной структурой

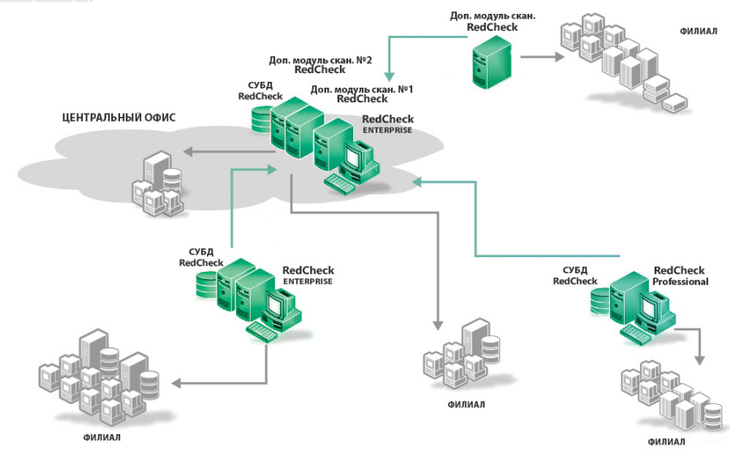
Для работы в крупных и распределенных корпоративных структурах, оптимальным решением является использование Web-консоли и центрального сервера управления, разворачиваемого в головном офисе или ЦОД компании. Администратор безопасности из web-консоли может подключиться и полноценно управлять любым находящимся в его организации экземпляром RedCheck.

Для установки недостающих обновлений, выявленных в процессе аудитов, может использоваться интегрированная со сканером надстройка над сервером обновлений – RedCheck WSUS Service и установленные на хостах агенты RedCheck Update Agent for Windows.



REDCHECK ENTERPRISE

Для больших ИС (более 2000 узлов) рекомендуется установка RedCheck в редакции Enterprise. RedCheck Enterprise – редакция, включающая в себя все имеющиеся функциональные возможности программы, не имеет лицензионных ограничений по количеству сканируемых узлов и ориентирована на крупные и распределенные информационные системы с возможностью неограниченного масштабирования.
Для масштабирования системы предусмотрено использование дополнительного модуля сканирования. Дополнительный модуль может устанавливаться на отдельный сервер или на тот же, на котором уже развернут RedCheck для повышения его производительности.



Для работы на небольших территориально удаленных объектах достаточно установки дополнительного модуля сканирования, подключаемого к экземпляру RedCheck Enterprise, установленному в центральном офисе или в одном из филиалов. Данные о результатах проверки сохраняются в единой БД, не создавая ощутимой нагрузки на каналы связи RedCheck. Для сбора и представления обобщенных данных из нескольких экземпляров RedCheck Enterprise предусмотрен консолидатор, включенный в комплект поставки.

При сканировании Windows-систем для сокращения нагрузки на сеть и снижения требований к привелигиям доступа к сканируемому узлу рекомендуется использование агента RedCheck. Использование агента не требует отдельного лицензирования и может использоваться совместно с имеющимися транспортами WMI или WinRM.

В общем случае максимальный состав системы RedCheck Enterprise может включать следующие структурные компоненты:

- основной экземпляр сканера (RedCheck Master);
- подчиненные экземпляры сканера (RedCheck Slave);
- дополнительные модули сканирования (ScanModule RedCheck);
- локальный сервер обновлений (Update Server RedCheck);
- консоль управления (Web-консоль RedCheck);
- модуль (надстройка) для MS WSUS (WSUS-сервис RedCheck);
- консоль управления MS WSUS и каталогами обновлений (WSUS-консоль RedCheck);
- консолидатор;
- агент сканирования Windows-систем (Agent RedCheck);
- агент установки обновлений для Windows-систем (Update RedCheck).

ИНТЕГРАЦИЯ С SIEM И СУИБ

RedCheck имеет готовые модули (коннекторы) для интеграции с такими СУИБ и SIEM-системами, как: HP ArcSight, Splunk, R-Vision, NEURODAT, eplat4m Security GRC. Использование типовых интерфейсов онлайн передачи данных для данного вида продуктов позволяет без особых проблем подключать и иные SIEM/СУИБ или подобные им системы.

Интеграция осуществляется через модуль API (REST-HTTP) или путем получения данных напрямую из базы данных RedCheck. Все данные структурированы, хранятся и передаются в формате XML.

Заложенные технические возможности позволяют не только передавать во внешние системы все полученные результаты проверок (типовая возможность большинства конкурентных продуктов), но и осуществлять управление RedCheck из внешних систем, в том числе создавать и запускать задания, формировать отчеты, дополнять базу сигнатур собственными, представленными в стандартизованном формате OVAL/XCCDF.

СЕРТИФИЦИРОВАННАЯ ВЕРСИЯ

Сканер безопасности RedCheck имеет действующий сертификат ФСТЭК России, который подтверждает соответствие средствам контроля (анализа) защищенности и требованиям 4 уровню отсутствия НДВ. Сканер может использоваться в составе АС до класса защищенности 1Г, а также ИСПДн, ГИС и АСУ ТП КВО до 1 класса (уровня) защищенности включительно.

RedCheck внесен в Единый реестр российских программ для электронных вычислительных машин и баз данных.

RedCheck может использоваться для реализации мер защиты согласно приказам ФСТЭК России № 17, 21, 31:

- Контроль за установкой компонентов программного обеспечения (ОПС.2);
- Сбор, запись и хранение информации о событиях безопасности (РСБ. 3);
- Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5);
- Выявление, анализ уязвимостей информационной системы (АН3.1);
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АН3.2);
- Контроль работоспособности параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АН3.3);
- Контроль состава технических средств, программного обеспечения средств защиты информации (АН3.4);
- Контроль состава технических средств, программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1);
- Контроль целостности виртуальной инфраструктуры и ее конфигураций (ЗСВ.7);
- Управление изменениями конфигурации информационной системы и системы защиты данных (УКФ.2);
- Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных (УКФ.4).

Также система может использоваться для реализации мер по обеспечению безопасности КИИ согласно приказу ФСТЭК России №239:

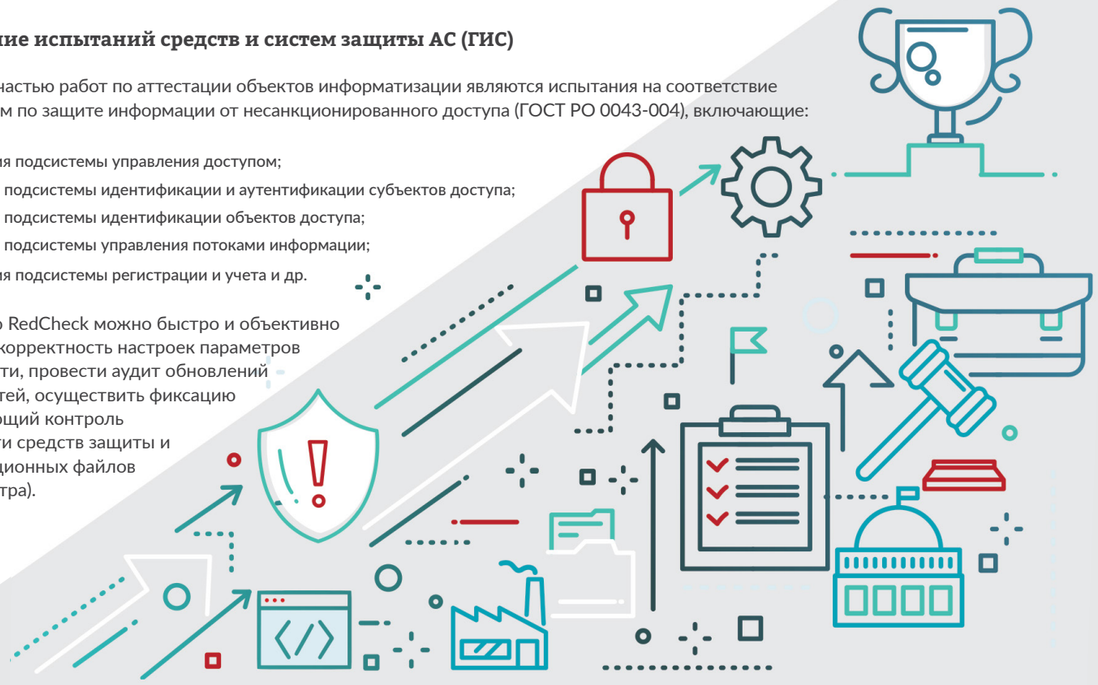
- Инвентаризация информационных ресурсов (АУД.1);
- Анализ уязвимостей и их устранение (АУД.2);
- Регистрация событий безопасности (АУД.4);
- Мониторинг безопасности (АУД.7);
- Проведение внутренних аудитов (АУД.10);
- Проведение внешних аудитов (АУД.11);
- Контроль целостности программного обеспечения (ОЦЛ.1);
- Контроль целостности информации (ОЦЛ.2);
- Идентификация объектов управления конфигурацией (УКФ.1);
- Управление изменениями (УКФ.2);
- Контроль действий по внесению изменений (УКФ.4);
- Поиск, получение обновлений программного обеспечения от доверенного источника (ОПО.1);
- Контроль целостности обновлений программного обеспечения (ОПО.2);
- Установка обновлений программного обеспечения (ОПО.4).

Проведение испытаний средств и систем защиты АС (ГИС)

Составной частью работ по аттестации объектов информатизации являются испытания на соответствие требованиям по защите информации от несанкционированного доступа (ГОСТ РО 0043-004), включающие:

- Испытания подсистемы управления доступом;
- Проверка подсистемы идентификации и аутентификации субъектов доступа;
- Проверка подсистемы идентификации объектов доступа;
- Проверка подсистемы управления потоками информации;
- Испытания подсистемы регистрации и учета и др.

С помощью RedCheck можно быстро и объективно проверить корректность настроек параметров безопасности, провести аудит обновлений и уязвимостей, осуществить фиксацию и последующий контроль целостности средств защиты и конфигурационных файлов (веток реестра).



СИСТЕМНЫЕ ТРЕБОВАНИЯ

ТИПОВЫЕ ТРЕБОВАНИЯ К АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

Редакция / Компонента	СУБД	Узлов не более	Аппаратные компоненты [1]	Частота сканирования		
				1 раз в неделю	1 раз в месяц	1 раз в квартал
RedCheck Base/Pro	MS SQL Express установлен на одном ПК с RedCheck	200	CPU	Intel Core i5-7400 (4 ядра) и выше		
			RAM	8 ГБ		
			HDD[1]	12 ГБ (10ГБ ограничение MS SQL Express)		
RedCheck Base/Pro	MS SQL Server (отдельный сервер)	200 и более	CPU	Intel Xeon E5 (не менее 2 физических ядер)		
			RAM	6 ГБ		
			HDD	2 ГБ		
		200	HDD [2]	21,8 ГБ	5,8 ГБ	2,6 ГБ
		500	HDD	53 ГБ	13 ГБ	5 ГБ
		2000				
RedCheck Enterprise	MS SQL Server (отдельный сервер)	-	CPU	Intel Xeon E5 (не менее 4 физических ядер)		
			RAM	6ГБ		
			HDD[1]	2 ГБ		
			HDD	400 ГБ	100 ГБ	35 ГБ
Дополнительный модуль сканирования (ScanModule RedCheck)	MS SQL Server (отдельный сервер)		CPU	Intel Xeon E5 (не менее 2 физических ядер)		
			RAM	6ГБ		
			HDD[1]	1ГБ		
			HDD	209 ГБ	49 ГБ	17 ГБ
Локальный сервер обновлений (Update Server RedCheck);	MS SQL Server (отдельный или совмещенный сервер)		CPU	Intel Xeon E5 (не менее 2 физических ядер)		
			RAM	6ГБ		
			HDD[1]	2 ГБ		
Агенты сканирования Windows-систем (Agent RedCheck) и установки обновлений (Agent Update RedCheck)			CPU	Intel Pentium/ AMD Phenom и выше		
			RAM	2 ГБ		
			HDD[1]	5 МБ		

[1] В таблице не указаны требования к аппаратной части операционной системы, на которой развернут RedCheck и СУБД. Параметры аппаратной платформы для операционной системы и MS SQL соответствует требованиям Microsoft.

[2] Расчет требуемого места на HDD приведен из условия хранения данных о результатах проверок - 1 год.

СРЕДНЯЯ НАГРУЗКА НА СЕТЬ ПРИ СКАНИРОВАНИИ ОДНОГО УЗЛА

	Способы / транспорты сканирования			
	Агент	Remote Engine (WinRM)	WMI	SSH
Скорость передачи данных, Кбит/с	121	637	10 200	160
Суммарный объем трафика на узел, КБ	32 000	16 800	434 000	5 000
Среднее время сканирования[1], мин	2,40	2,20	15,00	2,20

[1] Показатели приведены для режима «Аудит уязвимости, полное сканирование», данный режим является наиболее ресурсоемким.

Требования к программному обеспечению

Операционная система: Microsoft Windows 7-10, Microsoft Windows Server 2008-2016.

СУБД SQL Server 2012 (редакции Express, Standard, Enterprise).

Дополнительное программное обеспечение: Microsoft .NET Framework full версии 4.0 или выше.

ЛИЦЕНЗИРОВАНИЕ

Программа RedCheck лицензируется по количеству сканируемых (проверяемых) IP-адресов одной программой или по количеству инсталляций экземпляров программ. Для корпоративного использования предусмотрено четыре редакции программы RedCheck, отличающиеся функциональными возможностями:

REDCHECK BASE - младшая редакция продукта, включающая необходимые инструменты для полноценного аудита уязвимостей и обновлений Windows и Linux систем. Позволяет осуществлять контроль целостности, инвентаризацию, сетевые проверки и другие процедуры, необходимые при повседневном контроле защищенности информационных систем.

REDCHECK PROFESSIONAL – полнофункциональная редакция, включающая широкий арсенал инструментов для мониторинга и управления защищенностью сетей корпоративного уровня. Лицензируется по количеству сканируемых IP-адресов (DNS-имен).

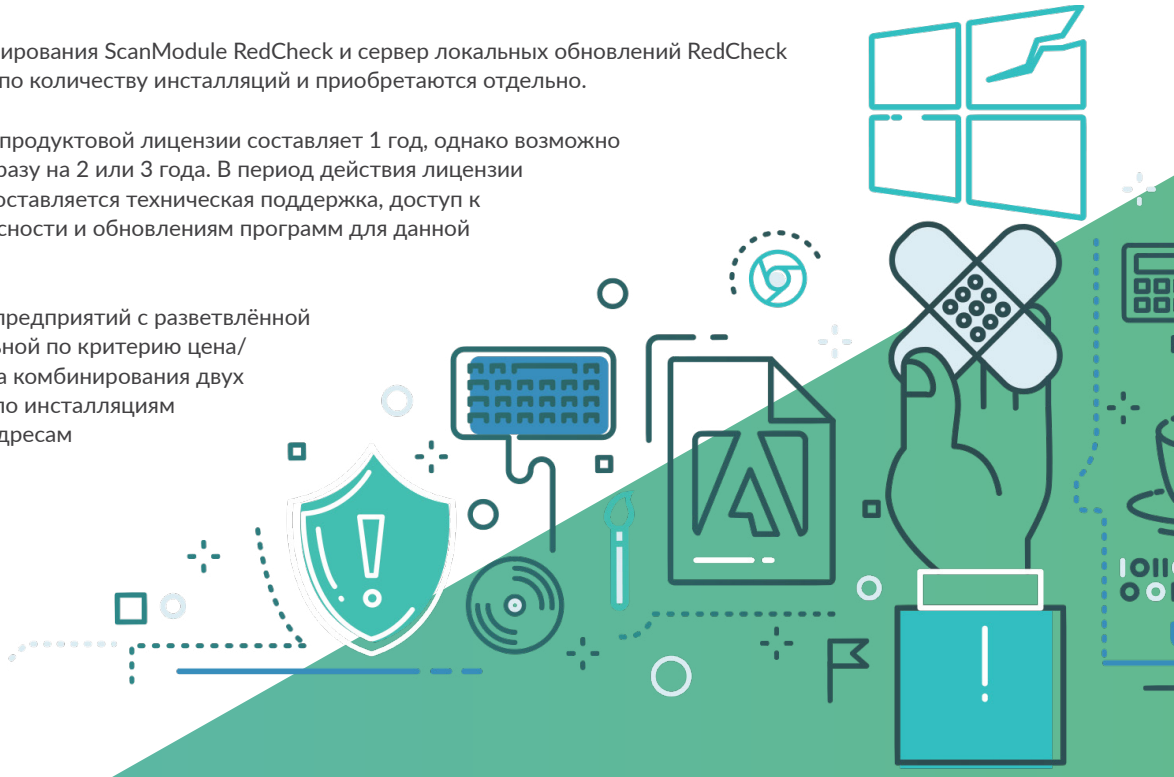
REDCHECK PROFESSIONAL ДЛЯ СЕРТИФИЦИРОВАННЫХ ВЕРСИЙ MICROSOFT – по своим возможностям программа аналогична редакции RedCheck Professional, но при этом дополнена возможностью управлять конфигурациями и установкой обновлений для сертифицированных по требованиям безопасности версий Microsoft. Редакция поставляется только пользователям сертифицированного программного обеспечения Microsoft.

REDCHECK ENTERPRISE – редакция включает все имеющиеся функциональные возможности программы и ориентирована на крупные и распределенные информационные системы с возможностью неограниченного масштабирования. Лицензируется по количеству инсталляций, не имеет ограничений на количество сканируемых IP-адресов. Для масштабирования возможно подключение дополнительных модулей сканирования (ScanModule RedCheck). Дополнительный модуль может устанавливаться на отдельный сервер или на тот же, на котором уже развернут RedCheck для повышения его производительности. В состав лицензии включена расширенная техническая поддержка.

Дополнительный модуль сканирования ScanModule RedCheck и сервер локальных обновлений RedCheck Update Server лицензируются по количеству инсталляций и приобретаются отдельно.

По умолчанию срок действия продуктовой лицензии составляет 1 год, однако возможно приобретение ПО RedCheck сразу на 2 или 3 года. В период действия лицензии пользователю RedCheck предоставляется техническая поддержка, доступ к актуальному контенту безопасности и обновлениям программ для данной версии.

Для крупных корпоративных предприятий с разветвлённой IT-инфраструктурой оптимальной по критерию цена/эффективность является схема комбинирования двух вариантов лицензирования – по инсталляциям (редакция Enterprise) и по IP-адресам (Professional).



ЗАО «АЛТЭКС-СОФТ»

141067, Московская обл., г. Королев, микрорайон Болшево, ул. Маяковского, д.10А

+7 (495) 543 31 01

redcheck.ru