

Dr.Web ATM Shield

<https://антивирус.рф>
<https://www.drweb.ru>

**Централизованная защита
встроенных компьютерных систем
(банкоматов, мультикиосков,
кассовых сетей и др.)**

- Полное соответствие закону №152-ФЗ «О персональных данных», а также другим документам регуляторов, предъявляемым к антивирусным продуктам для защиты систем работы с финансовыми средствами.
- Позволяет выполнить требования стандартов PCI-DSS v2 и v3, Федерального закона №161-ФЗ «О национальной платежной системе».
- Минимальные системные требования и малый расход трафика при обновлениях.



Шлюз – первый уровень защиты компании. От того, насколько он справится с атакой злоумышленников, может зависеть весь ее бизнес.

Dr.Web ATM Shield — это комплексный продукт централизованной информационной защиты, предназначенный для работы во встроенных компьютерных системах. Dr.Web ATM Shield легко интегрируется в сети банкоматов и кассовых устройств, позволяет не только защитить их от вредоносных объектов, но и существенно сократить время их обслуживания.

Использование уникальных технологий и наличие подробной документации позволяет провести развертывание антивирусного сервера и всей антивирусной сети в минимальные сроки. Система защиты может быть развернута практически в любой сети, вне зависимости от ее размера и особенностей — общего количества устройств и филиалов, используемой топологии, наличия сервера Active Directory, качества каналов связи.

Внедрение Dr.Web ATM Shield обеспечивает защиту от вредоносного ПО и снижает затраты на IT-подразделения.

Особенностью Dr.Web ATM Shield является возможность установки на устройства с небольшим объемом оперативной памяти и управления защитой из любой точки мира с одного компьютера, вне зависимости от используемой на нем операционной системы.

Ключевые особенности продукта

- Надежная защита банкоматов, терминалов, вендинговых устройств от проникновения всех типов вредоносного ПО.
- Защита устройств со «слабой» конфигурацией аппаратной части.
- Надежная работа в условиях наличия плохих линий связи.
- Минимальная совокупная стоимость продукта и снижение финансовых потерь.
- Развертывание защиты в день оплаты.
- Простота и удобство централизованного управления.
- Наличие подробной системы отчетов о состоянии сети.

Компоненты продукта

Веб-интерфейс администратора	•
Система информирования	•
Система контроля состояния защиты и сбора статистики	•
Централизованный карантин	•
Система антивирусного мониторинга	•
Защита от несанкционированных действий обслуживающего персонала	•
Система внутреннего аудита	•
Резервное копирование критически важных данных сервера защиты сети	•
Антивирусная защита от вредоносных программ любого типа	•

Dr.Web ATM Shield — это...

Выполнение требований регуляторов

Применение Dr.Web ATM Shield позволяет полностью выполнить требования стандартов PCI-DSS v2 и v3, Федерального закона N 161-ФЗ «О национальной платежной системе», а также иных законодательных актов в области антивирусной защиты.

Контроль изменений и удобная система отчетности

Антивирусная сеть, основанная на Dr.Web ATM Shield, обладает высокой прозрачностью работы. Журнал аудита действий администраторов позволяет отслеживать все шаги по установке и настройке системы. Любое действие над файлами, производимое компонентами антивирусной сети, отображается в отчете.

Надежная защита сетей любого размера и типа, в том числе и без доступа в Интернет

Непревзойденное качество лечения и высокий уровень самозащиты не дают вирусам и другим вредоносным объектам шанса проникнуть в защищаемую сеть. Использование новейших технологий и наличие глобальной системы вирусного мониторинга обеспечивает надежную защиту всех компонентов сети. «Горячие» обновления выпускаются немедленно после анализа новой вирусной угрозы. Благодаря компактной вирусной базе обновления проходят практически молниеносно.

Экономия трафика локальной сети

Dr.Web ATM Shield обеспечивает минимальный сетевой трафик, основанный на специально разработанном протоколе обмена информацией в сетях, построенных на основе протоколов TCP/IP, IPX и NetBIOS с возможностью применения специальных алгоритмов сжатия трафика. Экономия сетевого трафика обеспечивается специальным оптимизированным протоколом, поддерживающим компрессию данных между клиентом и сервером.

Сокращение финансовых потерь

Исключение вероятности заражения устройств сети снижает финансовые потери от простоя, необходимого для восстановления работоспособности системы.

Сохранение деловой репутации

Dr.Web ATM Shield не позволяет злоумышленникам получить контроль над устройством в результате его заражения с целью блокировки или вывода денежных средств.

Установка продукта в день платежа

Развертывание продукта проводится удобным для администратора способом — через политики Active Directory, стартовые скрипты, механизмы удаленной установки. Установка возможна, даже если узел сети является закрытым и недоступным для системы управления.

Минимальная стоимость

Dr.Web ATM Shield является комплексным продуктом — он включает все необходимые элементы защиты и единый центр управления. Системным администраторам не придется устанавливать множество различных программ, а сбор статистики происходит практически «одним кликом».

Удобство администрирования

Dr.Web ATM Shield содержит средства централизованного управления всеми компонентами антивирусной защиты встроенных систем, включая развертывание, обновление вирусных баз и программных модулей компонентов, мониторинг состояния всех защищенных узлов сети, получение уведомлений о вирусных инцидентах и настройки автоматической реакции на них, а также сбора статистики.

Веб-интерфейс администратора позволяет управлять защитой из любой точки Интернета или локальной сети, с любого компьютера. Он содержит средства планирования регулярных сканирований и обновлений вирусных баз и программных модулей, позволяет производить повседневную работу за считанные минуты: регулировать ключевые параметры антивирусных серверов и защищаемых объектов, изменять настройки и запускать задания на выполнение. Имеются возможности реализации политик безопасности, необходимых для конкретной сети и отдельных групп компьютеров, и назначения отдельных администраторов для различных групп. При необходимости можно сгруппировать несколько серверов Dr.Web ATM Shield с комплексной структурой взаимодействия между ними.

Использование Dr.Web ATM Shield позволяет минимизировать возможность проникновения вирусов на защищаемые устройства. Это является возможным благодаря:

- наличию технологий, позволяющих минимизировать время проверки и загрузку рабочей станции (в том числе за счет многопоточного сканирования и отложенной проверки файлов, открываемых «на чтение»), что обеспечивает стабильную работу системы даже на компьютерах с устаревшей конфигурацией;
- проверке файлов до начала использования их в соответствующих приложениях, что не дает возможности хакерам воспользоваться уязвимостями программного обеспечения;
- наличию современного антивирусного ядра, позволяющего находить и обезвреживать новейшие вирусы, еще не занесенные в вирусные базы, в том числе и скрытые под неизвестными упаковщиками;
- реализации мощной системы самозащиты, что не дает возможности вирусам вывести средства безопасности из строя.

Лицензирование Dr.Web ATM Shield

Виды лицензий

По числу защищаемых устройств

Все условия лицензирования: <https://license.drweb.ru/products/biz>

Предпродажная поддержка	Техническая поддержка
<ul style="list-style-type: none">Бесплатное тестирование продуктов Dr.Web — в сети заказчика или удаленно в виртуальной среде.Развертывание, помощь при внедрении — по телефону или с выездом на территорию заказчика (только в Москве).Презентация, вебинар, семинар.Помощь в написании или проверке написанного технического задания.Бесплатные обучающие курсы по администрированию продуктов Dr.Web	<ul style="list-style-type: none">Круглосуточно — по телефону и через форму https://support.drweb.ru.В России, на русском языке.Бесплатные услуги поддержки и бесплатная расшифровка от троянцев-вымогателей для лицензий в прайсовом диапазоне.Стоимость поддержки для запрашиваемых и безлимитных лицензий оговаривается особо.Платная VIP-поддержка.

Услуги и сервисы

Dr.Web vxCube

- Облачный интеллектуальный интерактивный анализатор подозрительных объектов на вредоносность
- Немедленное изготовление лечащей утилиты по результатам анализа
- Для специалистов по информационной безопасности и киберкриминалистов

Незаменимым средством в ситуациях, когда вредоносный файл пробрался внутрь защищаемого антивирусом периметра или у вас появились обоснованные, на ваш взгляд, подозрения, что в сети завелся «чужой», является облачный интерактивный анализатор Dr.Web vxCube.

Dr.Web vxCube в течение одной минуты оценит вредоносность файла и изготовит лечащую утилиту для устранения последствий его работы. Проверка занимает от одной минуты! По результатам анализа предоставляется отчет. Его можно просмотреть в личном кабинете пользователя Dr.Web vxCube или скачать в виде архива.

Если объект однозначно представляет угрозу, пользователь немедленно получает специальную сборку лечащей утилиты Dr.Web CureIt! (если это входит в лицензию) для очищения системы от действий, произведенных проанализированным файлом.

Это дает возможность максимально быстро обезвредить новейшую угрозу, не дожидаясь обновлений используемого антивируса.

Благодаря универсальности утилиты Dr.Web CureIt!, способной работать без установки в любой системе, где используется другой антивирус (не Dr.Web), это будет особенно полезно компаниям, пока не использующим Dr.Web в качестве основного средства защиты.

Демодоступ: <https://download.drweb.ru/vxcube>

Подробнее о Dr.Web vxCube: <https://www.drweb.ru/vxcube>

Антивирусные исследования

Анализ вредоносных файлов специалистами антивирусной лаборатории «Доктор Веб»

Ни один автоматизированный сервис никогда не заменит опыт и знания вирусного аналитика. В случае если вердикт Dr.Web vxCube о проанализированном файле будет не однозначно вредоносный, но у вас останутся сомнения в этом решении и, предлагаем воспользоваться услугами специалистов антивирусной лаборатории «Доктор Веб» с многолетним опытом вирусного анализа.

Услуги включают анализ вредоносных файлов любой сложности, по результатам которого выдается отчет, содержащий:

- описание алгоритмов работы вредоносного ПО и его модулей;
- категоризацию объектов: однозначно вредоносный, потенциально вредоносный (подозрительный), др.;
- анализ сетевого протокола и выявление командных серверов;
- влияние на зараженную систему и рекомендации к устранению заражения.

Заявки на антивирусные исследования принимаются по адресу: <https://support.drweb.ru>

Экспертиза вирусозависимых компьютерных инцидентов (ВКИ)

Если ваша компания пострадала от действия вредоносного ПО и требуется квалифицированная экспертиза вирусных аналитиков, воспользуйтесь услугами специального подразделения компании «Доктор Веб».

Об экспертизе ВКИ: <https://antifraud.drweb.ru/expertise>

Заявки на экспертизу: <https://support.drweb.ru/expertise>



© ООО «Доктор Веб», 2003–2019

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Тел.: +7 495 789-45-87 (многоканальный), факс: +7 495 789-45-97

<https://антивирус.рф> • <https://www.drweb.ru> • <https://free.drweb.ru> • <https://curenet.drweb.ru>

