vGate-S R2

Защита государственной тайны в виртуальной среде

Позволяет применять средства виртуализации в АС до 1Б

Позволяет автоматизировать работу администраторов по конфигурированию и эксплуатации системы безопасности

Способствует противодействию ошибкам и злоупотреблениям при управлении виртуальной инфраструктурой

Облегчает приведение виртуальной инфраструктуры в соответствие законодательству, отраслевым стандартам и лучшим мировым практикам

vmware PARTNER TECHNOLOGY ALLIANCE

Назначение

vGate-S R2 – сертифицированное средство защиты информации от несанкционированного доступа и контроля выполнения ИБ-политик для виртуальной инфраструктуры на базе платформ VMware vSphere 4 и VMware vSphere 5

Основные возможности

- **Защита информации от утечек через специфические каналы среды виртуализации**
- **Разделение объектов инфраструктуры на логические группы и сферы администрирования через мандатное и ролевое управление доступом**
- **Усиленная аутентификация, разделение ролей и делегирование полномочий**
- **Управление и контроль над конфигурацией системы безопасности**
- **Автоматическое приведение инфраструктуры в соответствие требованиям и постоянный контроль соответствия**

Код безопасности
ГК «Информзащита»

vGate-S R2

Защита государственной тайны в виртуальной среде

Виртуализация сегодня является одним из основных направлений развития информационных технологий. Перевод ИТ-инфраструктуры компании в виртуальную среду позволяет снизить расходы и повысить эффективность использования ИТ-активов компании. Вместе с тем обработка и защита информации в виртуальной среде имеют свои специфические особенности.

vGate-S R2 – средство защиты информации от несанкционированного доступа и контроля выполнения ИБ-политик для виртуальной инфраструктуры на базе платформ VMware vSphere 4 и VMware vSphere 5. vGate-S R2 облегчает приведение виртуальной инфраструктуры в соответствие законодательству, отраслевым стандартам и лучшим мировым практикам.

Использование vGate-S R2 помогает пройти аттестацию информационных систем, эксплуатируемых в виртуальной среде, в соответствии с российским законодательством.

Ключевые возможности

Мандатное управление доступом

- Разделение объектов инфраструктуры на логические группы и сферы администрирования с помощью бизнес-категоризации.
- Мандатный контроль доступа реализован двумя типами меток конфиденциальности:
  – иерархия уровней конфиденциальности.
  – метки бизнес-категорий информации.

Усиленная аутентификация, разделение ролей и делегирование полномочий

- Усиленная аутентификация администраторов, имеющих доступ к управлению конфигурацией.
- Для исключения «суперпользователя» создаются отдельные роли администратора ИБ и администратора ВИ.

Управление конфигурацией системы безопасности

Автоматическое приведение виртуальной инфраструктуры в соответствие положениям законодательства, отраслевых стандартов и лучших мировых практик:

- ФЗ-152.
- СТО БР ИББС.
- PCI DSS.
- VMware Security Hardening Best Practice.
- CIS VMware ESX Server Benchmark.

Контроль над изменениями настроек безопасности

Контроль над изменениями на основе заданных корпоративных политик безопасности.

Защита от утечек через специфические каналы среды виртуализации

- Контроль виртуальных устройств.
- Контроль целостности и доверенная загрузка виртуальных машин.
- Контроль доступа к элементам инфраструктуры.
- Согласование готовой виртуальной машины у администратора ИБ.
- Запрет доступа администраторов ВИ к данным виртуальных машин.

Мониторинг событий ИБ и создание структурированных отчетов

- Отчеты о текущем статусе конфигурации системы безопасности.
- Отчеты о произошедших событиях и изменениях.
- Отчеты о соответствии стандартам и лучшим мировым практикам.
- Регистрация попыток доступа к инфраструктуре.
- Интеграция с SIEM-системами.

Поддерживаемые платформы

- VMware vSphere 4.
- VMware vSphere 5.

Сертификат

Сертификат ФСТЭК России по ТУ и НДВ 2 дает возможность использовать продукт для защиты автоматизированных систем (АС) до класса 1Б включительно и информационных систем персональных данных (ИСПДн) до класса К1 включительно.

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Код Безопасности
ГК «Информзащита»

Тел.: +7 (495) 980-2345, E-mail: info@securitycode.ru
www.securitycode.ru