## **Требования к Системе**

### **Функциональные требования к Системе**

1. Техническое Решение может быть реализовано на базе программных решений, представляющих собой образ для инсталляции в корпоративную среду виртуализации, построенную на основе технологий VMware vSphere 6.5 или на основе программно-аппаратных комплексов, реализующих требуемый функционал.
2. Система должна иметь возможность подключения дополнительных подсистем: Web шлюз, E-mail security
3. Дополнительные подсистемы должны взаимодействовать с подсистемой DLP, тем самым усиливая её.

4. Поддержка работы Решения с почтовой системой Exchange для SMTP шлюзов.

5. Поддержка интеграции Решения с Active Directory (обязательно через TLS/SSL).

### **Требования к консоли администрирования**

1. Использование технологий Flash или Java апплетов не допускается.

2. Наличие ролевой модели доступа к интерфейсу управления с разграничением доступного функционала в зависимости от присвоенной пользователю роли. Возможность создание своих ролей доступа и назначения их пользователям Active Directory.

3. Наличие в консоли администрирования функционала журналирования и отчетности.

4. Консоль администрирования должна включать возможность делегированного доступа.

### **Требования к подсистеме отчетности и логирования.**

1. Подсистема журналирования должна включить следующие журналы:

a. Журнал подключений с указанием IP адресов

b. Аудит действий администратора

с. Журналы HTTP(s) соединений с указанием передаваемого трафика, пользователя инициирующего соединение, кода HTTP

d. Журналы ошибок возникающих в Системе

3. Подсистема отчетности должна предоставлять возможность генерации следующих отчетов:

a. Топ политик DLP по количеству инцидентов

b. Топ пользователей по количеству инцидентов DLP

4. Должна поддерживаться генерация отчетов в форматах: PDF, XLS, HTML.

5. Должна поддерживаться возможность генерации отчетов по расписанию.

6. Должна поддерживаться возможность получения отчетов по электронной почте согласно расписанию.

7. Должна быть возможность задания относительного или абсолютного временного промежутка, по которому генерируется отчет.

8. Должен вестись аудит действий администраторов.

9. Должен поддерживаться делегированный доступ к системе отчетности

### **Требования к компонентам DLP.**

1. Возможность выполнения DLP анализа на конечных устройствах, без необходимости передачи данных на стороннее устройство.

2. Наличие встроенной системы OCR для предотвращения утечки конфиденциальной информации в графических файлах.

3. Возможность настройки делегированного управления для разбора инцидентов DLP.

4. Регистрация конфиденциальных документов, хранимых в виде файлов.

5. Регистрация структурированных конфиденциальных данных, хранимых в таблицах реляционных СУБД.

6. Возможность работы Endpoint DLP работать с различными классификаторами, такими как машинное обучение, скрипты, цифровые отпечатки, регулярные выражения, словари, ключевые слова, свойства и типы файлов. Возможность работы Endpoint DLP для всех классификаторов должна поддерживаться как в режиме мониторинга, так и в режиме блокировки, в случае приобритения E-mail security так же должен поддерживаться карантин, для Endpoint DLP должно поддерживаться нативное шифрование чувствительного контента, передаваемого на сменные носители.

7. Обработка всех транзакций компонентами DLP должна осуществляться локально, без передачи на центральный сервер, сервера сторонних решений.

8. DLP компоненты должны иметь возможность передачи теневой копии файла или данных для которых происходит срабатывание по политикам DLP.

9. DLP политики должны быть едиными для всех компонентов DLP, либо Исполнителем должна быть реализована автоматизация процесса создания политик для каждого компонента DLP, таким образом, чтобы любые объекты политик (правила, классификаторы, действия) необходимо было описывать один раз.

10. В рамках подсистемы DLP должен быть модуль аналитики осуществляющий корреляцию событий, относящихся к одному инциденту, для минимизации сил, затрачиваемых оператором на расследование инцидента.

11. Производитель должен иметь интеграцию со своими модулями/сервисами защиты данных по каналам Интернет, электронная почта, сеть, конечные точки и облачные среду, файловые хранилища.

12. Система должна обнаруживать чувствительную информацию и в случае не правильного её хранения создавать инцидент.

13. Система должно имееть возможность применять политики вне сети.

### **Требования к endpoint агент**

1. Возможность аудита и блокировки транзакций по каналам:
2. Removable Media (отправка на USB носители)
3. Endpoint LAN (Сохранение на Сетевые каталоги)
4. Printing (Печать)
5. Application Control (Контроль приложений)
6. Endpoint Email (Контроль Outlook)
7. Endpoint Discovery (Обнаружение на узлах)

### **Компоненты подсистемы endpoint агент**

1. Автономность - Агент должен быть способен защищать при отключении от корпоративной сети и должен быть способен анализировать передаваемые данные в реальном режиме времени без необходимости обращения к дополнительным серверам для анализа.
2. Мониторинг и блокировку исходящего трафика в случае обнаружения несанкционированной отправки конфиденциальных данных.
3. Обнаружения конфиденциальных данных, в том числе и персональные данные.
4. Обнаружен конфиденциальных данных за счет предварительного механизма обучения по примерам конфиденциальных документов. При этом Агент должен обеспечивать обнаружение при использовании черновиков, модифицированных документов или их частей.
5. Распознавания неконфиденциальных бланков и форм от конфиденциальных документов, построенных на базе данных бланков и форм, различение конфиденциальных и неконфиденциальных документов построенных на базе одних и тех же бланков.
6. Обнаружение с возможностью последующей блокировки передачи файлов неизвестного/нестандартного формата.
7. Разграничения доступа к конфиденциальных данных по приложениям. Например, агент должен обладать опцией предоставления доступа к файлу с использованием офисного пакета программ, но запрещать доступ при попытке использования SCP клиента, архиватора, шифратора.
8. Безопасного обмена конфиденциальных данных при использовании съемных носителей. Если согласно бизнес процессам есть необходимость использования съемных носителей для обмена конфиденциальных данных – необходимо, не блокируя бизнес-активность, минизировать риски утечки конфиденциальных данных. Примером подобных ситуаций может быть необходимость обмена данными между сотрудниками, находящемися вне офиса компании.
9. Функционирование при использовании инфраструктуры VDI.
10. Анализа HTTP/HTTPS траффика с АРМ. При этом, агент не должен влиять на работу системного ПО, не используемого для передачи данных.
11. Анализ печати с АРМ на принтеры, как сетевые, так и физически подключенные к АРМ. При этом Система, в случае возникновения инцидента, должна предоставлять возможность администратору ИБ проанализировать исходный файл, отправленный на печать.
12. Анализ копирования файлов на сетевые папки. При этом, должна поддерживаться возможность указания файловых серверов куда копирование КИ разрешено.
13. Получения данных из Active Directory по источнику инцидента.
14. Анализа конфиденциальных данных, статично хранящихся на АРМ.
15. Единых политик контент-мониторинга.
16. Делегирования управления на базе принципа ролевого доступа, при этом его механизмы должны предоставлять возможность разграничения доступа к инцидентам исходя из учетных записей, групп и организационных подразделений Active Directory. Например, одному из администраторов ИБ может быть разрешено анализировать инциденты пользователей входящих в определенную группу Active Directory.
17. Анализа сработавших правил по данному инциденту.
18. Быстрого анализа части транзакции по которым сработали правила.

### **Требования к возможностям интеграции.**

1. Решение должно иметь возможность интеграции с SIEM.

2. Возможность передачи на SIEM следующей информации: IP адрес отправителя, почтовый адрес отправителя, почтовый адрес получателя, результат сканирования, имя файла вложения, хэш сумма файла вложения, URL адреса из тела письма с включенной информацией о категории URL. Для прокси шлюза должна передаваться информация о пользователе, группе, URL к которому происходило обращение, информация о том было ли заблокировано обращение, количества переданного трафика в рамках сессии.

3. Интеграция с Active Directory для аутентификации администраторов консоли управления или пользователей портала самообслуживания.

4. Поддержка работы Решения с почтовой системой Exchange.

### **Требования по работе с БД журналов**

1. Хранение журналов в базе данных SQL.

2. Поддержка доступа к СУБД с использованием TLS

3. Аутентификация доступа к СУБД с использованием доменной учетной записи Active Directory.

4. Возможность задания срока жизни данных в журналах. Автоматическое удаление старых данных

### **Требования к архитектуре**

1. Архитектура Решения должна предусматривать возможность горизонтального масштабирования за счет увеличения количество узлов в Решении.

2. Решение должно поддерживать механизмы ролевого доступа к компонентам системы.

### **Базовые требования**

1. Интерфейс управления Решения должен быть доступен только пользователям, прошедшим процедуру аутентификации.

2. Наличие возможности подключаться утверждёнными Службой Информационной Безопасности стандартными средствами к Microsoft Active Directory и получать из нее информацию о пользователях и их членстве в группах безопасности AD.

3. Независимость от обновлений ОС и прикладного ПО - при обновлениях сервис Решения должен продолжать работать, при изменении антивирусного ПО сервис не должен блокироваться, работа стандартизованных программных компонентов не должна препятствовать корректной работе сервиса.

4. Работа с компонентами Решения должна осуществляться только по шифрованным каналам, причём, как в веб-интерфейсе, так и при межсерверном взаимодействии.

5. Административные учётные записи используются только администраторами для осуществления работ по обслуживанию систем.

6. Наличие распределения прав доступа, в том числе и для административных доступов