ZECURION

DLP и системные требования: как справиться в эпоху перемен

Александр Куликов
Консультант по внедрению Zecurion

О КОМПАНИИ

20 ЛЕТ

Опыта в ИБ, из них 15 лет — на DLP-рынке

КЛИЕНТЫ

В России и за рубежом, более 10 тыс. компаний

ПАРТНЁРЫ

Широкая партнерская сеть в России и за рубежом

ENTERPRISE РЕШЕНИЕ

Работа в сетях с 200 000 сотрудников и более

ПРОДУКТЫ

DLP, SWG, Storage Security

ИМПОРТОЗАМЕЩЕНИЕ

Поддержка: Astra Linux, Red OS, Alt Linux, GosLinux

Реестр, сертификаты

ПРОДУКТОВАЯ ЛИНЕЙКА ZECURION

Zecurion DLP

Защита информации от утечек по сетевым (интернет, почта) и локальным (флешки, диски, гаджеты) каналам

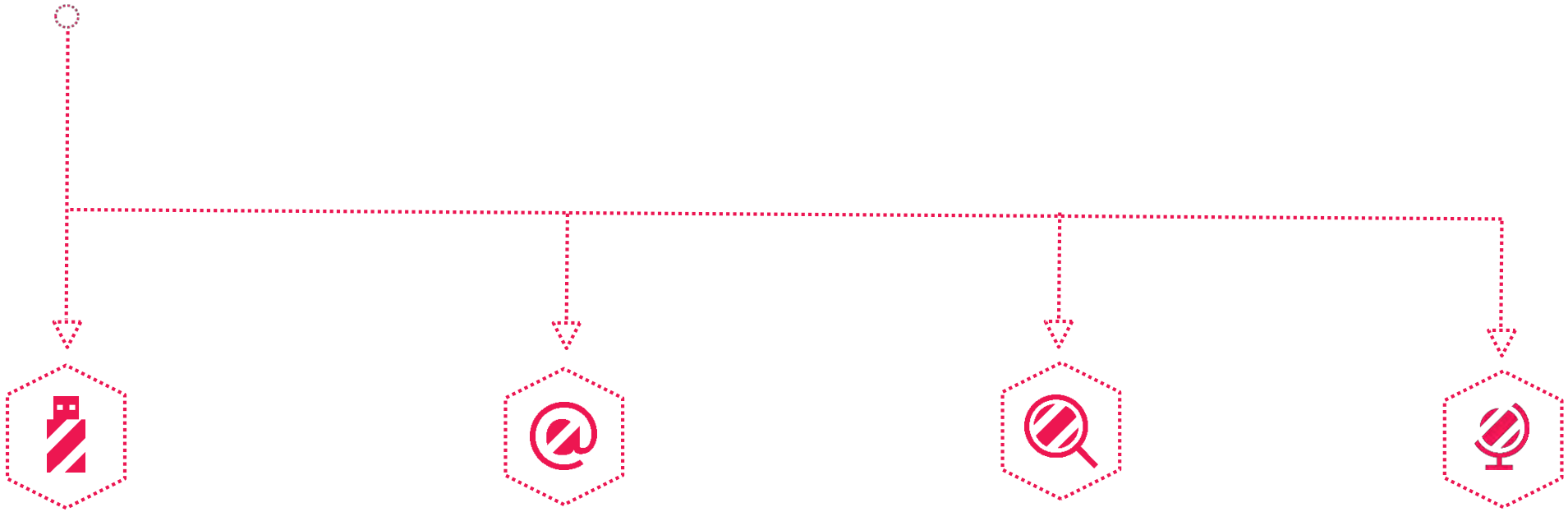
Zecurion SWG

В качестве прокси-сервера контролирует доступ сотрудников к веб-ресурсам и анализирует трафик, передаваемый по различным протоколам

Zecurion Staff control

Ведёт учёт рабочего времени и журналы действий сотрудников на рабочих местах, оценивает эффективность персонала

КОМПОНЕНТЫ ZECURION DLP



DEVICE CONTROL

Контролирует файлы, которые сотрудники распечатывают или копируют на USB, смартфоны и другие съёмные устройства

TRAFFIC CONTROL

Анализирует и блокирует любую информацию, пересылаемую за пределы локальной сети через почту, форумы или мессенджеры

DISCOVERY

Сканирует сервера и компьютеры, обнаруживает места хранения конфиденциальных данных

SWG

Используется в качестве собственного прокси-сервера

DEVICE CONTROL

- Разграничение доступа к любым устройствам на основе гибких политик
- Контроль всех копируемых на устройства данных и распечатаных на принтерах
- Архивирование всех записанных и распечатанных документов
- Превентивное теневое копирование
- Криптопериметр - принудительное шифрование файла при копировании на устройство
- Блокировка на основе контентного анализа содержимого файла

Устройства

- USB
- WiFi, Bluetooth
- DVD/CD
- Принтер
- Смартфон
- Порт LPT/COM
- Модем
- HDD
- FDD
- Ленточный накопитель
- Другие съёмные диски
- И т. д.

Снимки экрана

Буфер обмена

Клавиатура

Микрофон

Смарт-карта

Диск

Порт

TRAFFIC CONTROL

- Контетный анализ сетевого трафика
- Категоризация всей пересылаемой информации
- 10+ технологий обнаружения утечек, включая анализ графических файлов (OCR), цифровые отпечатки, самообучаемую технологию (SmartID) и пр.
- Контроль 500+ форматов файлов, 250+ веб-сервисов и 15+ IM
- Архив (теневое копирование) всей пересылаемой информации
- Превентивное теневое копирование

Email

- SMTP
- IMAP
- POP3
- MAPI

Web

- SMTP
- IMAP

Мессенджеры

- Telegram
- WhatsApp
- Mail.ru Agent
- MS Lync
- Skype
- Viber
- XMPP (Jabber)

Облачные хранилища

- OneDrive
- Dropbox
- Google Диск
- Яндекс.Диск
- Облако Mail.ru

Социальные сети

- Facebook
- ВКонтакте
- LinkedIn

DISCOVERY

- Сканирование в режиме реального времени всех сетевых и локальных хранилищ, в т. ч. рабочие станции и ноутбуки
- Автоматическое удаление найденных документов, не соответствующих политикам безопасности
- Категоризация всей перехваченной информации
- Готовые шаблоны конфиденциальной информации (50+ шаблонов)

Поддерживаемые хранилища

Локальные диски
Общие папки
MS SharePoint
MS Exchange
Любые базы данных, использующие ODBC

SWG

- Прокси-сервер
- URL-фильтрация
- Контентная фильтрация
- HTTPS-инспекция
- Access Log
- Контроль облачных хранилищ (CASB)
- Обнаружение вторжений (IDS)

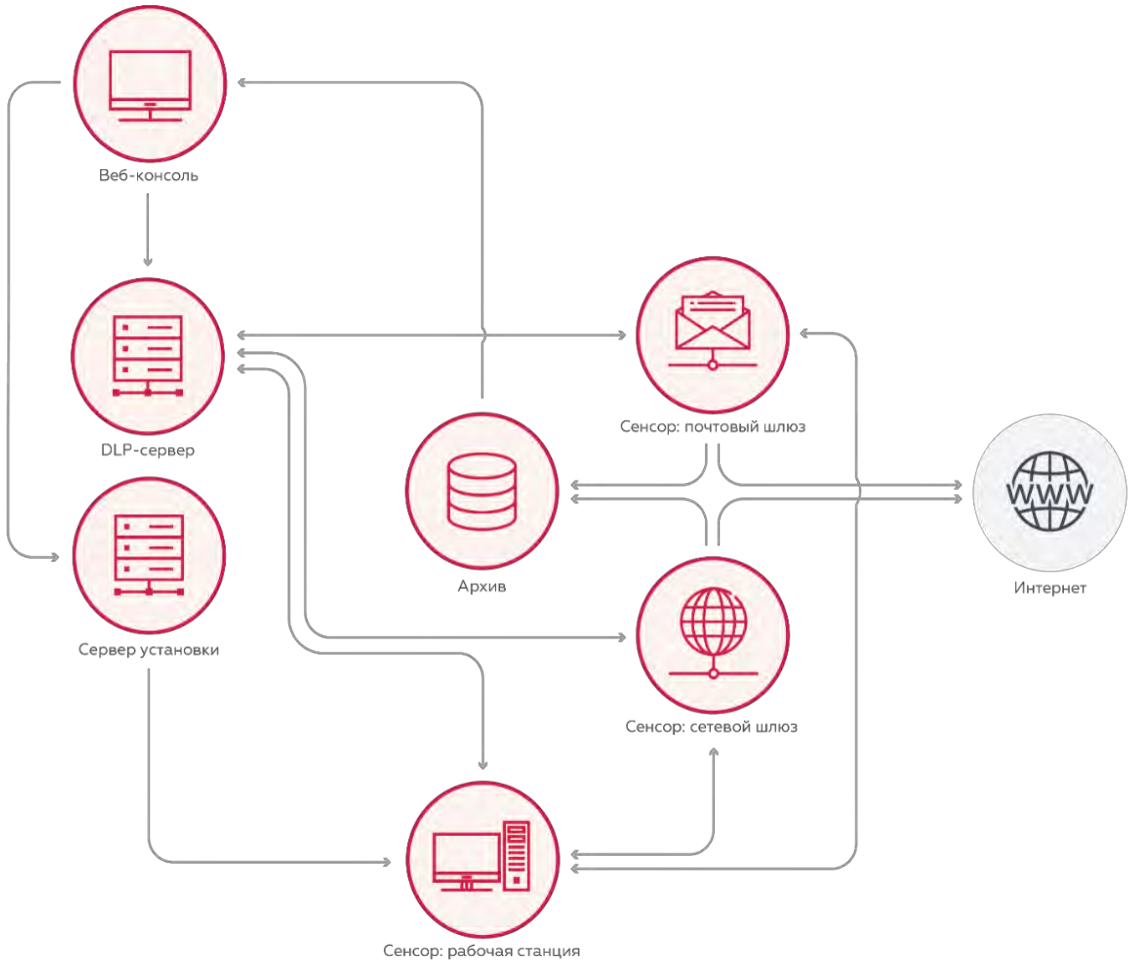
СВОДНАЯ ТАБЛИЦА ПО АППАРАТНЫМ ТРЕБОВАНИЯМ

DLP 1000	DLP5000	DLP10000	Для почты
Двухпроцессорный сервер (2*8 core); RAM от 16 Гб; HDD 200 Гб;	Двухпроцессорный сервер (2*12 core); RAM от 48 Гб; HDD 200 Гб;	Двухпроцессорный сервер (2*12 core); RAM от 128 Гб; HDD 200 Гб	Двухпроцессорный сервер (2*12 core) RAM от 24 Гб; HDD 100 Гб; 100 Гб (SSD); mail
Двухпроцессорный сервер (2*10 core); RAM от 24 Гб; HDD 100 Гб, 12 Тб (из расчета 100Мб в день на 1 пользователя);	СХД на 60 Тб (из расчета 100Мб в день на 1 пользователя)	Двухпроцессорный сервер (2*8 core); RAM от 48 Гб; HDD 100 Гб, 5 Tb	Двухпроцессорный сервер (2*24 core) RAM от 24 Гб; 200 Гб (SSD); ocr
	Двухпроцессорный сервер (2*12 core) RAM от 24 Гб; HDD 100 Гб; 100 Гб (SSD)	СХД на 120 Тб (из расчета 100Мб в день на 1 пользователя)	Двухпроцессорный сервер (2*24 core) RAM от 24 Гб; 200 Гб (SSD). ocr
	Двухпроцессорный сервер (2*12 core) RAM от 24 Гб; HDD 100 Гб; 100 Гб (SSD)	Двухпроцессорный сервер (2*12 core) RAM от 24 Гб; HDD 100 Гб; 100 Гб (SSD)	
	Двухпроцессорный сервер (2*24 core) RAM от 24 Гб; 200 Гб (SSD)	Двухпроцессорный сервер (2*12 core) RAM от 24 Гб; HDD 100 Гб; 100 Гб (SSD)	
		Двухпроцессорный сервер (2*12 core) RAM от 24 Гб; HDD 100 Гб; 100 Гб (SSD)	
		Двухпроцессорный сервер (2*12 core) RAM от 24 Гб; HDD 100 Гб; 100 Гб (SSD)	
		Двухпроцессорный сервер (2*24 core) RAM от 24 Гб; 200 Гб (SSD)	
		Двухпроцессорный сервер (2*24 core) RAM от 24 Гб; 200 Гб (SSD)	

ТРЕБОВАНИЯ К ПРОГРАММНО-АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

ZECURION DLP

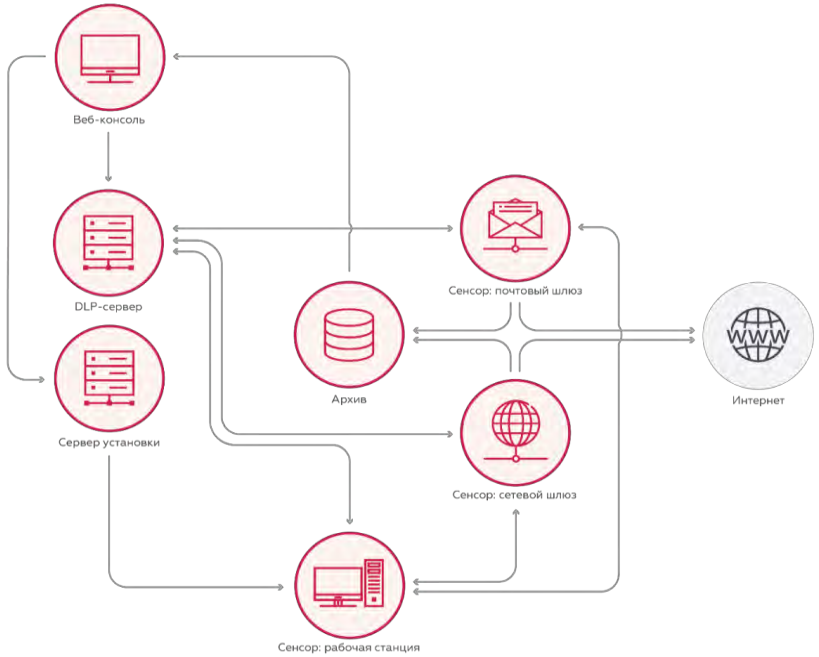
- Процессор: Intel Core и выше
- Достаточно одного сервера
- Оперативная память: 2 ГБ и выше
- Свободный объем на жестком диске: 5 ГБ
- Операционная система: Microsoft Windows Server 2008 R2 – 2019
- Microsoft SQL Server 2008 – 2019 или PostgreSQL 9.6, 10 или СУБД Jatoba— для сохранения инцидентов



ТРЕБОВАНИЯ К ПРОГРАММНО-АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

ZECURION TRAFFIC CONTROL

- Процессор: Intel Core и выше
- Достаточно одного сервера
- Оперативная память: 2 ГБ и выше
- Свободный объем на жестком диске: 4 ГБ + место для временного хранения писем
- Операционная система: Microsoft Windows Server 2008 R2 – 2019
- Прочие программные средства:

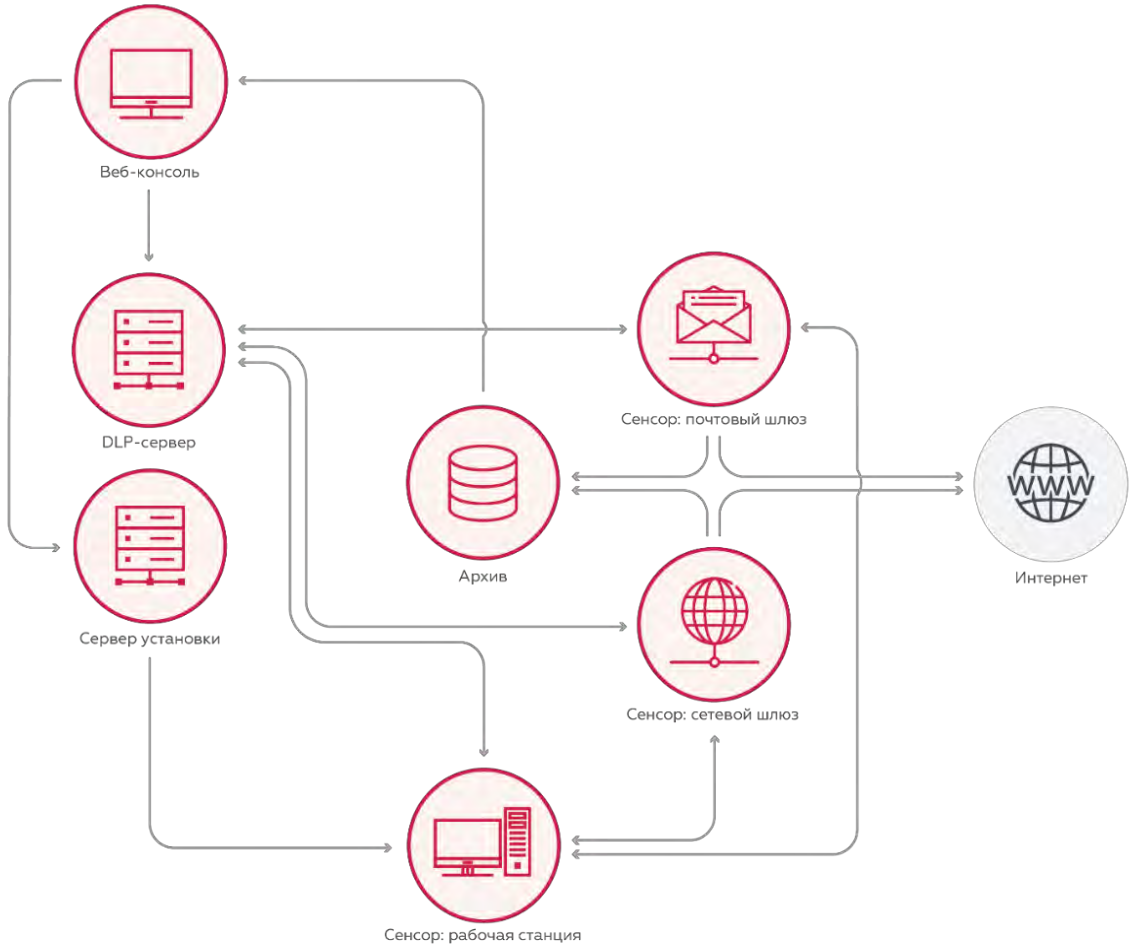


- ✓ Microsoft SQL Server 2008 – 2019 или PostgreSQL 9.6, 10, или СУБД Jatoba — для сохранения инцидентов.
- ✓ Microsoft Forefront TMG — для зеркалирования и фильтрации SSL-трафика (опционально).
- ✓ Microsoft Exchange 2007/2010/2013/2016 (x64) — для зеркалирования и фильтрации внутреннего почтового трафика Microsoft Exchange (опционально).

ТРЕБОВАНИЯ К ПРОГРАММНО-АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

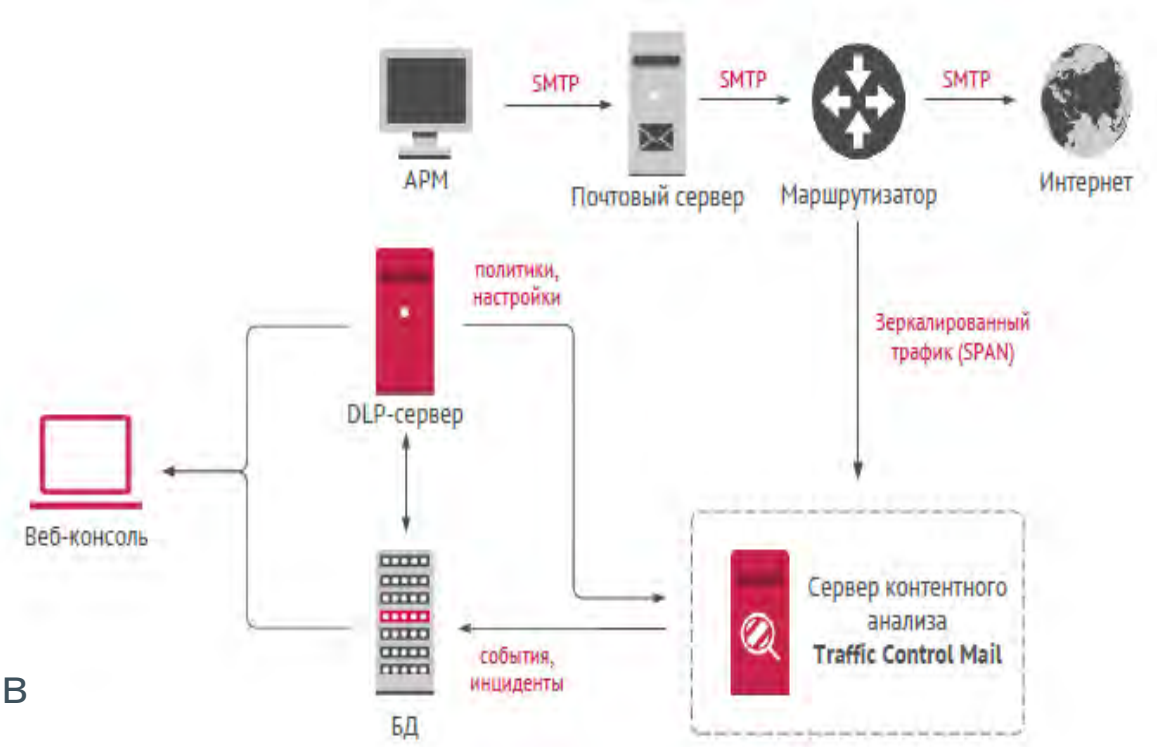
ZECURION NETWORK DISCOVERY

- Процессор: Pentium 4 и выше
- Достаточно одного сервера
- Оперативная память: 1 ГБ и выше
- Свободный объем на жестком диске: 5 ГБ
- Операционная система: Microsoft Windows Server 2008 R2 – 2019
- Прочие программные средства:
- Microsoft SQL Server 2008 – 2019 или PostgreSQL 9.6, 10, СУБД Jatoba — для сохранения инцидентов.



ВОЗМОЖНЫЕ РЕЖИМЫ РАБОТЫ ZECURION TRAFFIC CONTROL MAIL

- В качестве агента к транспортной службе (выполняющий роль Hub Transport) Microsoft Exchange
- Режим зеркалирования
- Режим анализа зеркалированного трафика
- Отдельный сервер в режиме сбора почты по протоколу POP3\HTTPS\IMAP4 из технологического п/я
- Отдельный сервер в разрыв между почтовым сервером и шлюзом
- Отдельный сервер в режиме анализа SMTP-журналов
- Установка Zecurion Traffic Control Endpoint (как плагин к почтовому клиенту OUTLOOK)на клиентские ПК с указанием сервера Zecurion DLP для получения конфигурации



РЕЖИМЫ РАБОТЫ ZECURION TRAFFIC CONTROL WEB/SWG

- режим анализа зеркалированного трафика
- режим ICAP-сервера
- режим фильтра к указанным протоколам (на сервере с TMG)
- Traffic Control Endpoint на клиентских ПК с указанием сервера Zecurion DLP для получения конфигурации

ZECURION

КОНТАКТЫ

+7 (495) 221-21-60
info@zecurion.com
www.zecurion.ru