Опыт внедрения и обслуживания систем ИБ

Антон Миносьян
Ведущий инженер отдела системной интеграции
aminosjan@polikom.ru

ПОЛИКОМ ПРО

Поставка ПО и оборудования
ИТ-инфраструктура
Бизнес-приложения
ЦОД, сети, инженерная инфраструктура

Комплексные системы

- Системы антивирусной защиты
- Защита веб-шлюза
- Защита Email-шлюза
- DLP

Система защиты корпоративной сети на базе Symantec Endpoint Protection (SEP)

Исходные данные

- ***Крупная компания – сотовый оператор и разработчик мобильного ПО***
- ***Порядка 800 рабочих мест, охваченных проектом (HQ и удаленные площадки)***
- ***“Зоопарк” неуправляемого стороннего антивирусного ПО (старые модули SEP, ЛК, F-Secure, и т.д.)***
- ***Система управления конфигурациями отсутствует (как в контексте КСАВЗ, так и в контексте всей ИС)***

SEP. Внедрение с настройкой “под ключ”

Полная настройка конфигураций и документирование

- *Развертывание и настройка серверных модулей и системы оповещений*
- *Формирование требований для эксплуатации в различных подразделениях компании и на их основании – всех необходимых политик управления конечными точками*
- *Политики – клиент (8), брандмауэр (6), IPS (6), управление приложениями и устройствами (7), обновление (2), исключения (3)*
- *Разработка комплексных сценариев развертывания клиентов и миграция с ПО сторонних вендоров с использованием имеющихся средств*
- *Специфические сценарии в ИС клиента*
  - *Мобильные рабочие места, расположения (location)*
  - *Citrix VDI*
- *Документирование по результатам*
  - *Развернутое техническое описание, инструкции/регламенты для администраторов и пользователей, руководство для ИТ-персонала по действиям при внештатной ситуации*

SEP. Сопровождение

Абонентское сопровождение с момента внедрения

- ***Ежедневный мониторинг состояния системы с коррекцией при необходимости***
- ***Порядка 115 нетривиальных кейсов по технической поддержке в собственной корпоративной системе SD***
- ***Взаимодействие с ТП вендора от имени заказчика. Подобное ПО следует покупать только с поддержкой!***
- ***Проактивное реагирование на инциденты, связанные с антивирусной безопасностью***
- ***Ни одной вирусной эпидемии за 4 с лишним года сопровождения. Пример с WannaCry***

SEP. Использование и перспективы

Выполнение обновления версий серверного и клиентского ПО в рамках ТП

- ***Поддержка новых версий клиентских ОС (Windows), обновленные антивирусные движки***
- ***Миграция на Symantec Endpoint Protection 14 (ранее использовался SEP 12 RU6)***

Использование системы для решения смежных задач, связанных с ИБ

- ***Выполнен проект по общему повышению защищенности рабочих мест, включая VDI. Наряду со сторонними технологиями (Windows SRP, настройка фильтрации вредоносных кодов на почтовой системе, контроль трафика на сетевом оборудовании), задействованы и штатные функции SEP (контроль устройств и приложений)***

Комплексная система защиты шлюза на базе Forcepoint Security

Исходные данные

- ***Крупный банк с основными офисами в Санкт-Петербурге и Москве, два датацентра***
- ***Порядка 3000 рабочих мест, охваченных проектом***
- ***Разнородные многокомпонентные решения для контроля на шлюзах***
  - ***Blue Coat на веб-шлюзе***
  - ***McAfee в качестве системы email-фильтрации***
  - ***Symantec DLP для защиты от утечек***
  - ***Продукты различаются идеологически, нет единой точки контроля за решением***
- ***Потребность в унификации***

Решение. Forcepoint Web/Email/Data/Endpoint Security

Виртуальная реализация

- ***Отказоустойчивые VM на кластерах VMware в обоих ЦОД (шлюзы CentOS, управление под Windows)***

Архитектура

- ***Размещение компонент в обоих ЦОД***
- ***Дополнительная кластеризация веб-шлюзов (2x2), почтовых шлюзов (1x2) и системы управления (1x2), собственными средствами Forcepoint***
- ***Модули DLP на конечных точках (Endpoint Security)***
- ***Единая точка контроля (веб-консоль с SSO на системе управления, к которой подключены все компоненты решения)***

Упрощение конфигурации

- ***В результате внедрения удалось сократить число VM с нескольких десятков до 10, и отказаться от “железок” (Blue Coat)***

Forcepoint Security. Используемые функции

Веб шлюз

- *Веб-прокси с контролем доступа (интеграция с LDAP)*
- *Антивирус, контентный фильтр/анализатор содержимого в веб-канале*
- *URL-фильтр с обновляемой базой данных категорий (Websense best-in-class), политики*
- *Два кластера из двух VM “активный-активный” в двух ЦОД*
- *Интеграция с DLP в канале веб на шлюзе*

Почтовый шлюз

- *Антивирус в email-канале*
- *Антиспам и контентные фильтры, управление на основе политик*
- *Возможность организации пользовательского карантина*
- *Отказоустойчивость (кластерный узел в каждом ЦОД, балансировка на два Интернет-канала)*
- *Интеграция с DLP в канале Email на шлюзе*

Forcepoint Security. Используемые функции (продолжение)

DLP

- ***Модуль Endpoint Security на конечных точках - контроль клиентов в каналах веб, почтовом, сетевом, печати и сменных носителях***
- ***Система контроля, классификации и поиска конфиденциальных данных в локальной сети, с возможностями машинного и ручного обучения***
- ***Отдельные модули распознавания текста (OCR на VM) для всех каналов, в реальном времени***

Система управления

- ***Кластеризована в режиме “активный-пассивный” (два ЦОД)***
- ***Единая точка управления (Web/Email/Data Security), SSO с интеграцией с LDAP***
- ***Отчетность по запросам и по расписанию, предопределенные шаблоны по всем компонентам***
- ***Оповещения***
- ***Интеграция с системой SIEM (Arcsight)***

Forcepoint. Внедрение с настройкой “под ключ”

Полная настройка конфигураций и документирование

- ***Развертывание и настройка VM***
- ***Формирование требований для политик веб, email фильтрации и DLP и их реализация. Система отчетности согласно бизнес-требованиям***
- ***Развертывание агентских компонент на клиентах с помощью имеющихся средств управления (Symantec Altiris)***
- ***Перевод нагрузки на новые шлюзы, демонтаж старых***
- ***Документирование по результатам***
  - ***Развернутое техническое описание, инструкции/регламенты для администраторов и пользователей, руководство для ИТ-персонала***

Forcepoint Security. Сопровождение

Сопровождение

- ***Ежедневный мониторинг состояния системы с коррекцией при необходимости. Анализ журналов ОС и ПО***
- ***Порядка 70 нетривиальных кейсов по технической поддержке в собственной корпоративной системе SD за полтора года, более чем по 2/3 с участием вендора***
- ***Взаимодействие с ТП вендора от имени заказчика, в том числе с привлечением инженеров по удаленным сессиям. Аналогичная ремарка про обязательную покупку ТП (Forcepoint без нее и не продается)***
- ***Ввиду бизнес-особенностей системы, основная реакция на внутренние инциденты – силами подразделения ИБ клиента***
- ***“Стресс-тестирование”. К произошедшим недавно эпидемиям ransomware (WannaCry, Petya) система оказалась изначально устойчивой - защита уже была к моменту начала активной фазы***
  - ***Требования аккуратно обновлять операционные системы никто и никогда не отменит!***
  - ***Контроль актуальности патчей входит в регламент сопровождения***

Forcepoint. Использование и перспективы

- **Выполнение обновления версий ПО в рамках ТП**
  - **Модули HF**
  - **В ближайшей перспективе – миграция на версию 8.4.0**
- **Рассматривается вариант подключения дополнительного функционала Forcepoint Advanced Malware Detection (https://www.forcepoint.com/product/cloud-security/forcepoint-advanced-malware-detection)**

Особенности эксплуатации в крупных средах

- Работа на “пересечении” технологий
  - Citrix (VDI)
  - VMware (виртуализация)
  - Microsoft (виртуализация, SQL, операционная система)
  - Сетевое оборудование
  - Общие вопросы (SQL, TCP/IP, UNIX, почтовые системы)
- Работа с несколькими вендорами при решении проблем
  - Необходимость правильной изоляции проблемы
- Взаимодействие с ИТ, а не только с ИБ подразделениями клиента

Благодарю за внимание!

Антон Миносьян
Ведущий инженер отдела системной интеграции
aminosjan@polikom.ru

ПОЛИКОМ ПРО

Москва
тел. (495) 660 32 91
факс (495) 660 32 93

Санкт-Петербург
тел. (812) 325 84 00
факс (812) 320 56 86

www.polikom.ru