Семейство решений HP ArcSight

Содержание:

Обзор решений HP ArcSight

Семейство продуктов HP ArcSight является лидирующим решением в области мониторинга и управления событиями информационной безопасности. По результатам ежегодных отчетов Gartner Magic Quadrant для решений по информационной безопасности (SIEM) HP ArcSight ESM шесть лет подряд занимает первое место.

Продукты HP ArcSight предназначены для сбора, обработки, корреляции и реагирования на события информационной безопасности. Решения, построенные на базе продуктов ArcSight, обладают свойствами масштабируемости, надежности, расширяемости и отказоустойчивости. Они обеспечивают возможность ежеминутной обработки нескольких сотен тысяч событий безопасности.

Продукты HP ArcSight также могут быть использованы для обеспечения соответствия требованиям международных стандартов, таких как PCI DSS, SOX, ISO 27001 и др.

Благодаря использованию продуктов HP ArcSight пользователь получает:

- Единую консоль, куда стекаются абсолютно все события информационной безопасности в компании любого размера, что дает возможность получить полную картину состояния информационной безопасности в компании, сопоставлять события и реагировать на них максимально быстро, поддерживать соответствие состояния информационной безопасности внутренним регламентам и внешним стандартам, таким как PCI DDS, SOX и т.д.
- Возможность приводить события безопасности, приходящие с различных устройств и программных решений, к единому виду, что делает возможным их упорядоченное хранение, сопоставление и корреляцию.
- Возможность автоматически выделять из сотен тысяч событий только те, которые несут в себе угрозу информационной безопасности, благодаря мощному корреляционному анализу событий, что позволит сконцентрировать силы специалистов по безопасности только на значимых событиях и минимизировать ложные срабатывания.
- Возможность централизованно хранить события информационной безопасности со всех устройств и программных решений в течение любого необходимого срока, что дает возможность осуществлять анализ долгосрочных трендов, а также обращаться к этой информации в любое время для поиска и анализа кибератак, ускорения проверок контролирующими органами, помощи в улучшении качества информационных услуг.

Состав семейства решений HP ArcSight

HP ArcSight ESM

Ядром линейки HP ArcSight является HP ArcSight ESM (Enterprise Security Manager). Данный продукт обеспечивает сбор, обработку и хранение событий безопасности, которые могут поступать из различных источников. Платформа HP ArcSight ESM обеспечивает взаимосвязанную инфраструктуру, способную определить каждое событие, поместив его в рамки контекста того, кем или чем оно вызвано, где, когда и почему произошло, а также, каково его влияние на бизнес риски.

Дополнительно к ресурсной модели HP ArcSight ESM, новейшая версия продукта включает в себя особую пользовательскую модель, работа которой основана на учете и контроле всех идентификаторов, ролей и групп пользователей, а также всех используемых в организации учетных записей. Данная пользовательская модель позволяет администратору соотнести такие общие идентификаторы, как адреса электронной почты, логины и учетные записи и составить отчеты обо всех действиях, произведенных пользователях в рамках системы, с помощью приложений, учетных записей и IP-адресов.

HP ArcSight ESM поддерживает интеграцию с максимальным количеством прикладных систем и устройств и поставляется с несколькими тысячами предустановленных правил корреляции.

HP ArcSight Connectors

Данные модули осуществляют сбор, нормализацию и категоризацию событий информационной безопасности перед отправкой их в HP ArcSight ESM. Благодаря HP ArcSight SmartConnector события, поступающие в HP ArcSight ESM, уже приведены к единому стандарту и определены в ту или иную категорию, что ускоряет их последующую обработку, сопоставление и корреляцию. Модули SmartConnector по умолчанию поддерживают сбор и нормализацию событий с более чем 300

различных устройств и систем. И помимо этого модуль FlexConnector позволяет легко при помощи мастера реализовать сбор и нормализацию данных из самописных и неподдерживаемых устройств и приложений.

HP ArcSight Console, Web и Viewer

Данные модули необходимы для настройки, администрирования и просмотра информации в HP ArcSight ESM.

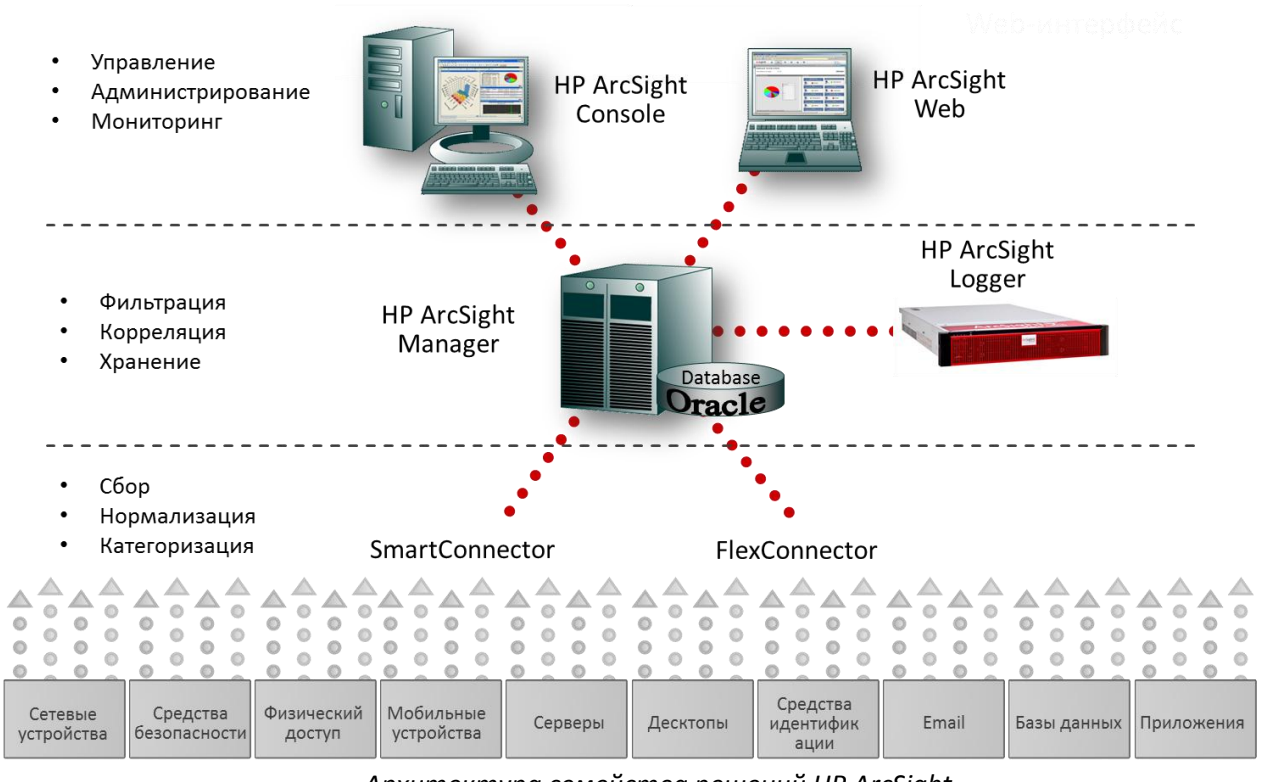
- Console – это клиентский модуль для управления HP ArcSight ESM, требующий установки на ПК пользователя. Интерфейс Console гибко настраивается под нужды конкретного пользователя.
- Web – аналог Console, работающий через web-браузер, что дает возможность удаленного управления системой без необходимости установки ПО на ПК пользователя, но обладает меньшей гибкостью в плане настройки пользовательского интерфейса.
- Viewer – Доступ к интерфейсу HP ArcSight ESM через web-браузер, предназначенный только для просмотра информации и составления отчетов, без возможности внесения изменений в настройки системы.

HP ArcSight Logger

Решение для долгосрочного хранения и управления информацией о событиях безопасности. Благодаря удобной системе поиска можно быстро найти и отсортировать интересующие события безопасности, сформировать подробный отчет за любой временной промежуток. Помимо этого долгосрочное хранение событий безопасности позволяет привести ИТ-безопасность в соответствие с корпоративными политиками и внешними стандартами.

HP ArcSight Express

Сбалансированный программно-аппаратный комплекс для быстрого развертывания, содержащий в себе функционал HP ArcSight ESM и HP ArcSight SmartConnectors. HP ArcSight Express уже включает в себя наиболее распространенные правила, сигналы тревоги и отчеты для контроля периметровой и внутрисетевой безопасности. Все средства заранее сконфигурированы и готовы к использованию. Благодаря этому решению даже компании с небольшим штатом IT-специалистов и специалистов по безопасности могут позволить себе организовать полноценную защиту сети от атак хакеров, вирусов, вредоносных программ, утечки информации и несанкционированного доступа.



Архитектура семейства решений HP ArcSight

Конкурентные преимущества

1. **Лидирующее решение в области мониторинга и управления событиями безопасности (SIEM).** Наибольшая доля рынка SIEM по отчетам IDC. Первое место среди SIEM решений на протяжении 6 лет по данным Gartner.
2. **Наиболее широкий набор возможностей по мониторингу и управлению событиями информационной безопасности.** Весь необходимый функционал в одном решении: от сбора событий и приведения их к единому стандарту, до ее обработки и долговременного хранения с удобным поиском по любым параметрам. А также преднастроенные комплекты правил для контроля соответствия международным стандартам.
3. **Беспрецедентные возможности масштабирования, доказанные на практике.** Уже есть реализованные проекты, где HP ArcSight ESM справляется с обработкой нескольких десятков миллионов событий безопасности в день!
4. **Наиболее широкий спектр поддерживаемых устройств и приложений.** На данный момент разработаны коннекторы для более чем 300 устройств и приложений более чем 200 вендоров. Благодаря FlexConnector SDK можно создать коннектор для приложений и устройств, не входящих в этот список.
5. **Выбор варианта приобретения.** Благодаря возможности приобретения решения в виде ПО или же преднастроенного программно-аппаратного комплекса, заказчик может выбрать решение наиболее точно удовлетворяющее его текущим потребностям, не переплачивая за невостребованные мощности. Возможность апгрейда позволит быстро нарастить производительность тогда, когда это будет необходимо.
6. **Возможность упрощенного развертывания и управления.** Благодаря HP ArcSight Express пользователь сразу получает готовое к работе решение с преднастроенным набором самых распространенных правил, сигналов тревоги и отчетов. Данное решение позволяет реализовать полноценный мониторинг и управление событиями безопасности даже в компаниях с небольшим штатом IT-специалистов и специалистов по безопасности.

Примеры получаемой информации

Благодаря централизованному сбору и стандартизации событий безопасности HP ArcSight ESM и HP ArcSight Express позволяет пользователю получать множество различных отчетов о состоянии тех или иных аспектов информационной безопасности. В комплект поставки входит некоторое количество преднастроенных отчетов и шаблонов. В дополнение к предустановленным отчетам и шаблонам среда позволяет пользователю создавать свои отчеты и шаблоны для специализированного и регулярного контроля.
Вот пример некоторых из них:

Отчеты уровня предприятия

- Основные показатели полосы пропускания
- Внесение изменений в конфигурацию
- Успешные и отклоненные запросы на доступ к системе
- Изменение паролей
- Основные нарушители и внутренние объекты атак

Отчеты о работе сетевых устройств

- Ошибки и критические события в работе сетевых устройств
- Сообщения о статусе и неработоспособности сетевых устройств
- Загрузка канала
- Внесение пользователем изменений в конфигурацию и смена типа
- Успешные и отклоненные запросы на доступ к системе
- Основные соединения

Отчеты по антивирусной защите

- Основные зараженные системы
- Все ошибки антивирусной защиты
- Статистика обновлений вирусных сигнатур
- Общая активность вирусов
- Внесение изменений в конфигурацию антивирусов

Отчеты баз данных

- Ошибки и предупреждения баз данных
- Успешные и отклоненные запросы на доступ к базам данных
- Внесение изменений в конфигурацию баз данных

Отчеты по системам обнаружения и предотвращения вторжений (IPS/IDS)

- Сигналы тревоги с информацией о параметрах работы IPS/IDS
- Количество сигналов тревоги
- Основные источники и адресаты сигналов тревоги
- Основные нарушители и внутренние объекты атаки

Отчеты об управлении доступом

- Аутентификация пользователей на всех основных узлах
- Успешные и отклоненные запросы на аутентификацию
- Внесение изменений в конфигурацию системы управления пользователями

Отчеты об устройствах виртуальной частной сети (VPN)

- Ошибки аутентификации в VPN
- Количество соединений
- Продолжительность соединений
- Принятые и отклоненные запросы на установление соединения
- Успешные и отклоненные запросы на доступ к системе
- Основные соединения
- Основные пользователи широкополосной сети
- Внесение изменений в конфигурацию VPN

Отчеты операционной системы

- Управление привилегированными пользователями
- Успешные и отклоненные запросы на доступ к системе
- Внесение изменений в конфигурацию

Отчеты межсетевого экрана

- Отклоненные входящие соединения
- Отклоненные входящие соединения
- Загрузка канала
- Успешные и отклоненные запросы на доступ к системе

С помощью функции детализации можно без труда перейти от общего отчета к конкретному инциденту по одному клику мышки на графике или диаграмме.

Лицензирование и варианты поставки

HP ArcSight ESM

Поставляется в виде программного решения или в виде программно-аппаратного комплекса.

Программное решение:

- Лицензируется по количеству ядер ЦП, которые будут задействованы для работы HP ArcSight ESM
- Производительность масштабируется за счет количества задействованных ядер ЦП
- Можно приобрести лицензии как в комплекте с правами на использование базы данных Oracle для хранения данных HP ArcSight ESM, так и без них. Второй вариант подразумевает наличие у заказчика «свободных» лицензий на БД Oracle
- Для покупки лицензий на второй сервер с целью построения отказоустойчивой системы предусмотрена скидка от стандартной цены
- Программные коннекторы SmartConnector входят в поставку в неограниченном количестве

Программно-аппаратный комплекс:

- Сервер для монтажа в серверную стойку с предустановленным ПО HP AcrSight ESM на базе ОС Linux
- Производительность зависит от выбранной модели программно-аппаратного комплекса. Различие моделей заключается в количестве ядер, задействованных для работы HP ArcSight ESM Manager (2 или 4 ядра). Возможен программный апгрейд между моделями
- Включает в себя базу данных Oracle для хранения данных HP ArcSight ESM
- Для покупки второго сервера такой же модели с целью построения отказоустойчивой системы предусмотрена скидка от стандартной цены

- Программные коннекторы SmartConnector входят в поставку в неограниченном количестве

HP ArcSight Connector

Поставляется в виде программного решения или в виде программно-аппаратного комплекса.

Программное решение:

- Устанавливается на оборудование заказчика
- HP ArcSight SmartConnector поставляется в комплекте с HP ArcSight ESM и HP ArcSight Express в неограниченном количестве

Программно-аппаратный комплекс:

- Сервер для монтажа в серверную стойку с предустановленным ПО HP ArcSight SmartConnector на базе ОС Linux
- Приобретается отдельно
- Как правило, используется для сбора данных в филиалах, кэширует данные и оптимизирует их передачу по WAN-каналам

FlexConnector SDK для разработки коннекторов к самописным и неподдерживаемым приложениям приобретается отдельно!

HP ArcSight Console, Web и Viewer

- HP ArcSight Console – клиентское приложение для управления и администрирования HP ArcSight ESM, требующее установки на ПК пользователя. Интерфейс гибко настраивается под нужды конкретного пользователя, что позволяет иметь перед глазами только те данные, которые необходимы в данный момент.
- HP ArcSight Web – доступ ко всем функциям управления и администрирования HP ArcSight ESM через web-браузер. По функционалу аналогичен HP ArcSight Console, но возможности настройки интерфейса под нужны пользователя несколько ограничены.
- HP ArcSight View – доступ к функциям мониторинга и составления отчетов через web-браузер без возможности внесения изменений в настройки HP ArcSight ESM.
- Все модули приобретаются по количеству пользователей, требующих тот или иной тип клиентского доступа

HP ArcSight Logger

Поставляется в виде программного решения или в виде программно-аппаратного комплекса

- Модели и редакции различаются производительностью, а также объемом хранимых данных
- Существуют как модели программно-аппаратных комплексов, хранящие данные на собственном массиве из локальных жестких дисков в отказоустойчивой конфигурации (RAID5), так и модель предусматривающая хранение данных в SAN

HP ArcSight Express

Поставляется **только** в виде программно-аппаратного комплекса для монтажа в серверную стойку. Поставка включает одну лицензию HP ArcSight Console и неограниченное количество программных SmartConnector.

Спецификации моделей HP ArcSight Express:

Model	AE7405	AE7410	AE7425	AE7450	AE7465	AE7480
Max Devices	750	750	750	750	1500	1500
Peak EPS/Flows	500/50K Flows	1,000/50K Flows	2,500/50K Flows	5,000/50K Flows	10,000/50K Flows	15,000/50K Flows
Max Assets	5,000	5,000	10,000	10,000	25,000	25,000

System OS	Red Hat Enterprise Linux 5 64-bit
Web Users	Unlimited
CPU	2 x Intel Xeon E5620 Quad Core 2.4 GHz
Interfaces	4 x 10/100/1000
RAM	36GB
Storage	6 x 600GB - SAS disks in RAID-10
Chassis	2U
Power	2x 750W CS Platinum 100-240 VAC
Dimensions	27.3"x 17.6"x 3.4"

Возможен апгрейд между моделями HP ArcSight Express, а также апгрейд до HP ArcSight ESM.

Техническая поддержка

К лицензиям и программно-аппаратным комплексам обязательно приобретается техническая поддержка минимум на 1 год. Техническая поддержка дает право на получение программных обновлений к приобретенным решениям, а также возможность обращения в службу технической поддержки вендора для разрешения проблем, возникающих в процессе использования решения.

Варианты технической поддержки:

- 9x5, 1 год (обращение в службу техподдержки в рабочие часы по будним дням)
- 24x7, 1 год (возможность круглосуточного обращения в службу техподдержки по будним и выходным дням)

Примеры использования

Заказчик: T-Mobile

Информация о заказчике:

- Один из лидирующих операторов мобильной связи в мире.
- Более 119 млн. клиентов в Европе и США, более 320 роуминг-партнеров в 130 регионов по всему миру.
- Один из первых операторов мобильной связи, внедривший передовые стандарты GPRS, UMTS

Проблемы заказчика:

- Множество разрозненных решений по мониторингу безопасности, управляемых вручную разными командами специалистов
- Отсутствие общей картины IT безопасности, обновляемой в режиме реального времени
- Невозможность корреляции событий
- Невозможность контролировать угрозы со стороны инсайдеров

Почему HP ArcSight ESM:

Решение было принято после детального исследования рынка и тестирования продуктов нескольких вендоров.

HP ArcSight ESM был единственным продуктом, который удовлетворил всем требованиям:

- Полная интеграция с существующей разрозненной инфраструктурой
- Богатые возможности корреляции

- Гибкость и масштабируемость решения
- Поддержка соответствия стандарту Sarbanes-Oxley (SOX)

Результаты внедрения HP ArcSight ESM:

- Возможность наблюдать, контролировать и отвечать на угрозы в режиме реального времени
- Технические специалисты освободились от часов низкоуровневого анализа, что позволило им сконцентрироваться на повышении IT безопасности
- Соблюдение соответствие стандарту SOX

Заказчик: Commerzbank

Информация о заказчике:

- Второй по размеру банк в Германии, с представительствами в более чем 40 странах и 35000 сотрудников
- Более 8 млн. клиентов по всему миру

Проблемы заказчика:

- Более 700 устройств, которые нуждаются в мониторинге безопасности
- Более 15 млн. событий безопасности каждый день (межсетевые экраны, прокси-серверы, IDS/IPS, антивирусы)
- События безопасности анализировались вручную без возможности охватить все события и их сопоставить

Почему HP ArcSight ESM:

Решение было принято после детального исследования рынка и тестирования продуктов 5 вендоров.
HP ArcSight ESM был единственным продуктом, который удовлетворил всем требованиям:

- Полная интеграция с существующей инфраструктурой
- Наиболее зрелые возможности корреляции и составления отчетов
- Масштабируемость в соответствии с потребностями бизнеса

Результаты внедрения HP ArcSight ESM:

- Возможность фильтровать и коррелировать миллионы событий безопасности каждый день
- Технические специалисты освободились от часов низкоуровневого анализа, что позволило им сконцентрироваться на повышении IT безопасности
- Полная картина событий безопасности

Дополнительные материалы

Информация на английском языке по продуктам HP ArcSight:

- HP ArcSight ESM
- HP ArcSight Connectors
- HP ArcSight Logger
- HP ArcSight Express
- Отчет Gartner Magic Quadrant for Security Information and Event Management 2010

Ознакомительные версии продуктов HP ArcSight

Для получения ознакомительных версий продуктов HP ArcSight обращайтесь на hp@axoft.ru