Hewlett Packard
Enterprise

Управление событиями информационной безопасности

Enterprise Security Products

Ляшенко Анастасия
Product Manager

IT Guard

Современные проблемы информационно безопасности:

- **Большое количество разнородных устройств безопасности**
  - **90%** используют межсетевые экраны и антивирусы
  - **40%** используют системы обнаружения вторжений (IDS)
  - количество сетевых устройств растет
  - больше оборудования означает большую сложность
- **Очень много событий по безопасности !**
  - один межсетевой экран может генерировать за день более 1 Гигабайта данных в Log-файле
  - один сенсор IDS за день может выдавать до 50 тыс. сообщений, до 95% ложных тревог!
  - сопоставить сигналы безопасности от разных систем безопасности практически невозможно.

Слишком много устройств, слишком много данных…

Ответные действия на угрозы безопасности должны быть предприняты немедленно!

Hewlett Packard Enterprise

IT Guard

HP ArcSight ArcSight

Платформа для мониторинга и оценки рисков ИБ

- Дает полную картину безопасности
- Анализирует события в реальном времени и дает необходимые знания на что реагировать
- Реагирует, чтобы предотвратить потери
- Оценивает эффективность работы людей и технологий

Архитектура решения HP ArcSight

- Управление
- Администрирование
- Мониторинг

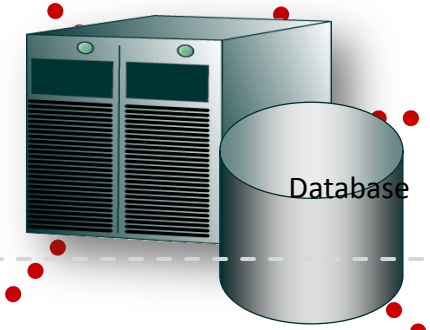
HP ArcSight Console

HP ArcSight Web

HP ArcSight Logger

- Фильтрация
- Корреляция
- Хранение

HP ArcSight ESM



- Сбор
- Нормализация
- Категоризация

SmartConnector

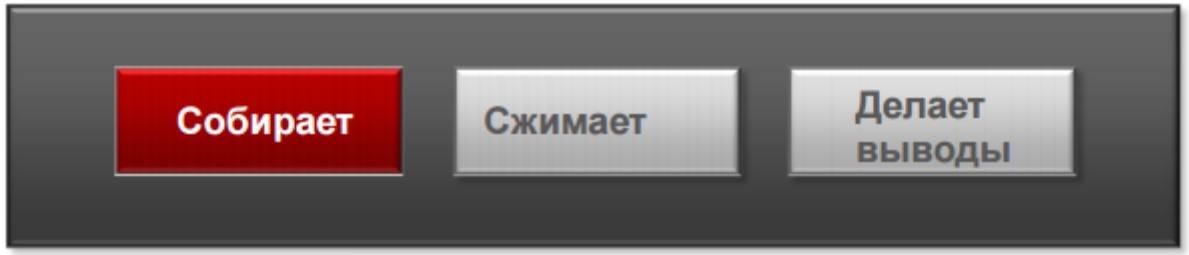
FlexConnector

Сетевые устройства	Средства безопасности	Физический доступ	Мобильные устройства	Серверы	Десктопы	Средства идентификации	Email	Базы данных	Приложения

Hewlett Packard Enterprise

IT Guard

ArcSight делает три вещи лучше чем другие:



Сбор событий в компании

- С любого утройства собираем события
- Собирает как есть в виде строк, либо разбивает и категоризирует данные
- Переводит в другой тип данных для анализа

Очень много качественных коннекторов

Access and Identity	Data Security	Integrated Security	NBAD	Policy Management	Vulnerability Mgmt
Anti-Virus	Firewalls	Log Consolidation	Network Management	Router	Web Cache
Applications	Honeypot	Mail Filtering	Network Monitoring	Security Management	Web Filtering
Content Security	Host IDS/IPS	Mail Server	Net Traffic Analysis	Switch	Web Server
Database	Network IDS/IPS	Mainframe	Operating System	VPN	Wireless

Нормализация

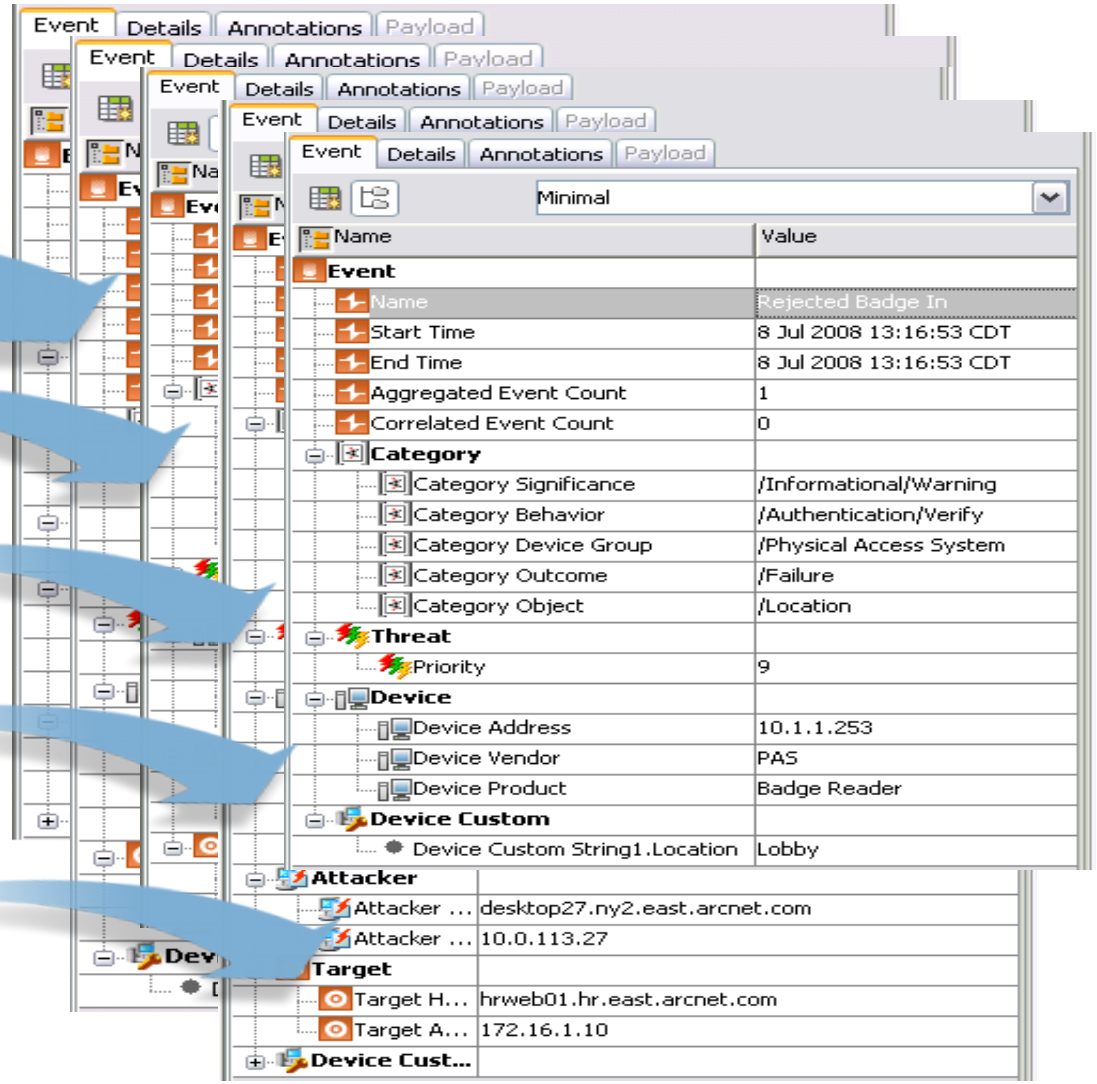
OS/390
Ошибка входа

UNIX
Ошибка входа

Oracle
Ошибка входа

Windows
Ошибка входа

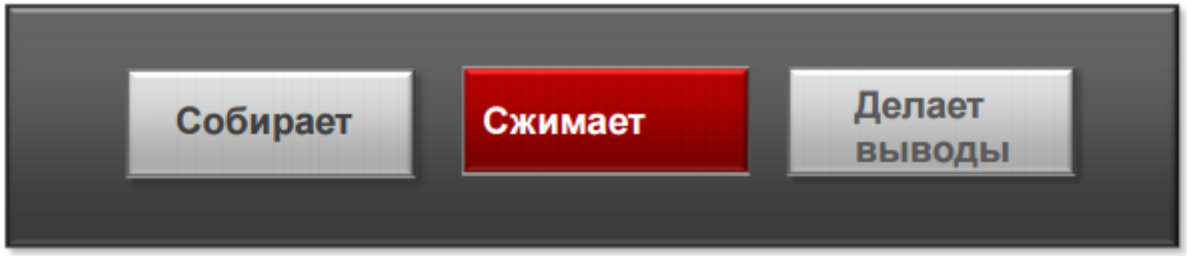
HID-карты
Вход запрещён



Hewlett Packard Enterprise

IT Guard

ArcSight делает три вещи лучше чем другие:



Сбор событий в компании

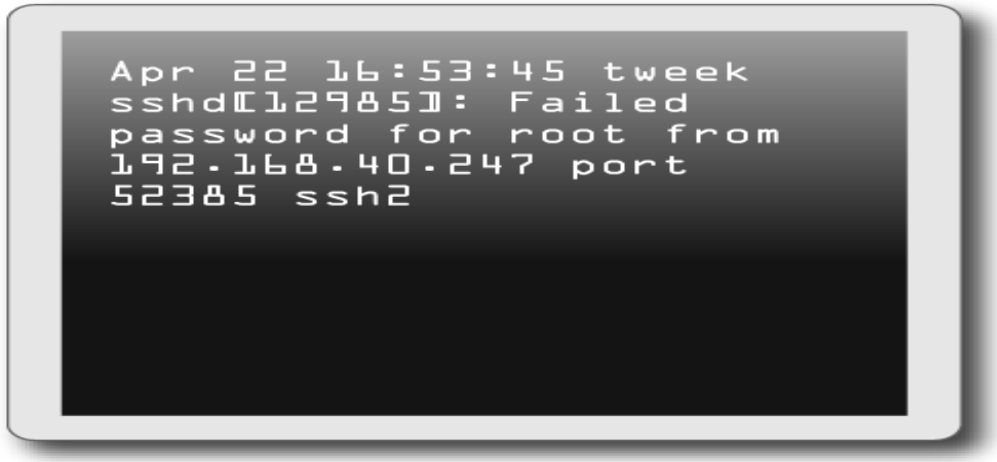
- Управление любыми данными для обеспечения безопасности, работы ИТ или соответствия требованиям
- Поиск и отчетность по данным за много лет
- Снижение затрат на хранение и простое управление петабайтами данных

Одно решение для всех журналов компании

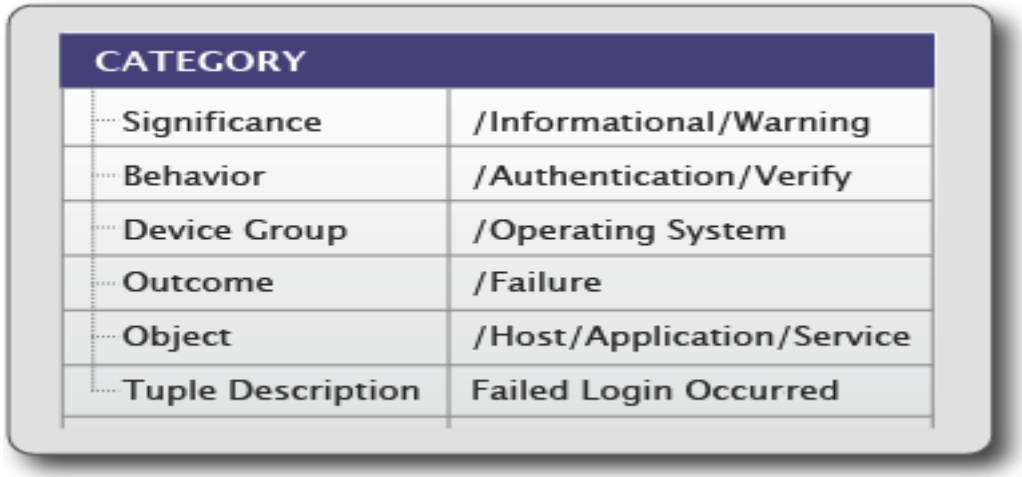
Категоризация

- Общая модель событий для всех устройств и программ
- Возможность понять действительную важность событий от различных систем
- Анализ событий независимо от типа устройства

Без категоризации



Категоризированное событие



Хранение

Компактно

За большой промежуток времени

Быстрый доступ

Сжатие 10 x

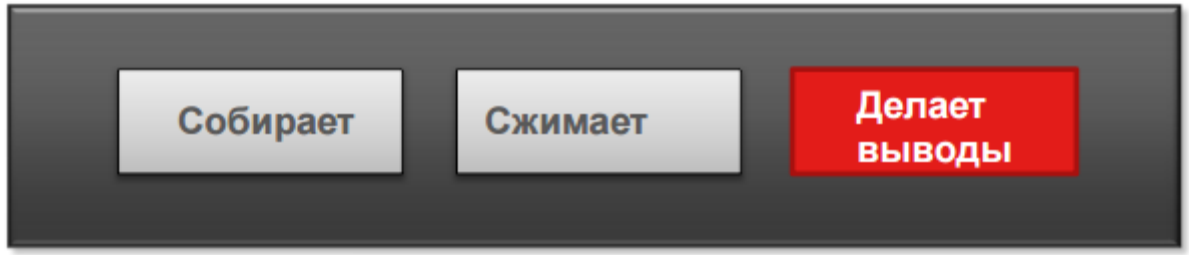
Хранилище 42 TB

Скорость поиска миллионы EPS

Hewlett Packard Enterprise

IT Guard

ArcSight делает три вещи лучше чем другие:

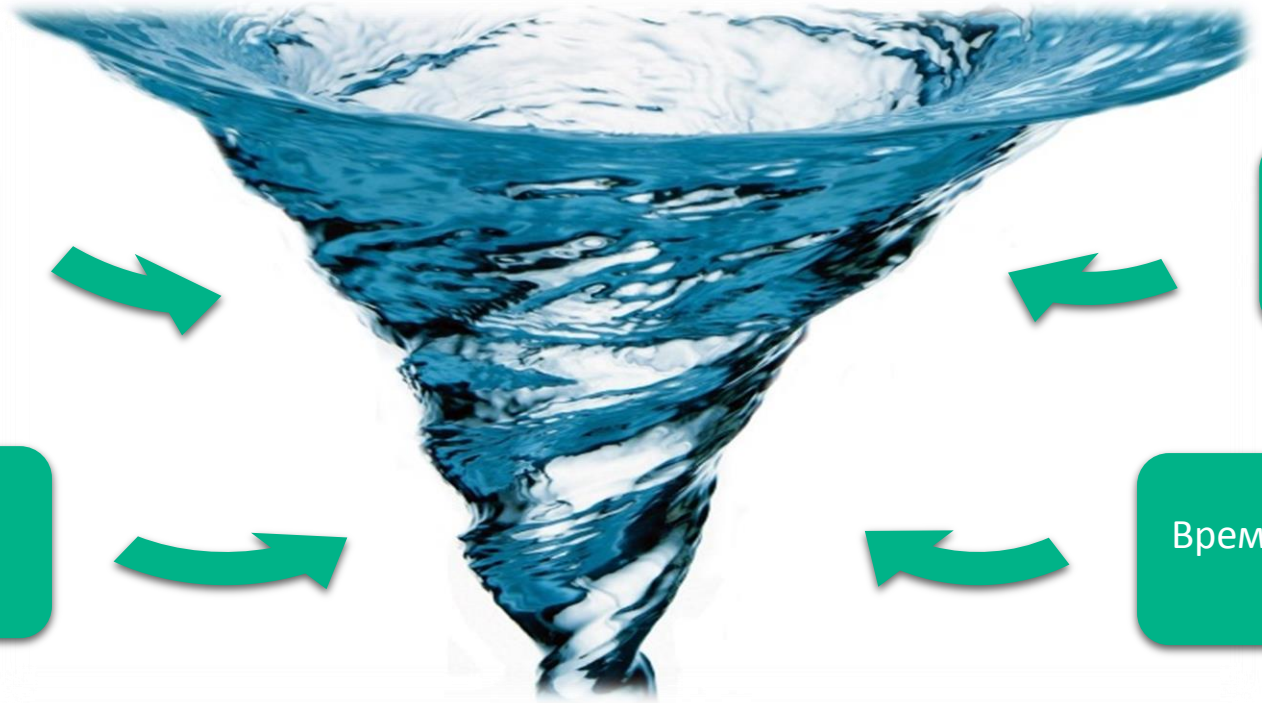


Корреляция

Корреляция

Кто:
Личность пользователя

Что:
Значимость актива



Где:
Контекстный анализ

Когда:
Временной промежуток

От миллионов событий до тех, что действительно важны!

Hewlett Packard Enterprise

IT Guard

Лицензирование

Пакет решений HPE Enterprise Security:

HPE ArcSight ESM/Express

HPE Logger/ Security Data Platform

HPE ArcSight SmartConnectors

Compliance Insight Packages

HPE ArcSight ThreatDetectors/ HPE ArcSight User Behavior

HPE AtcSight Reputation Security Monitor

HPE Management Center

HPE ArcSight ESM:

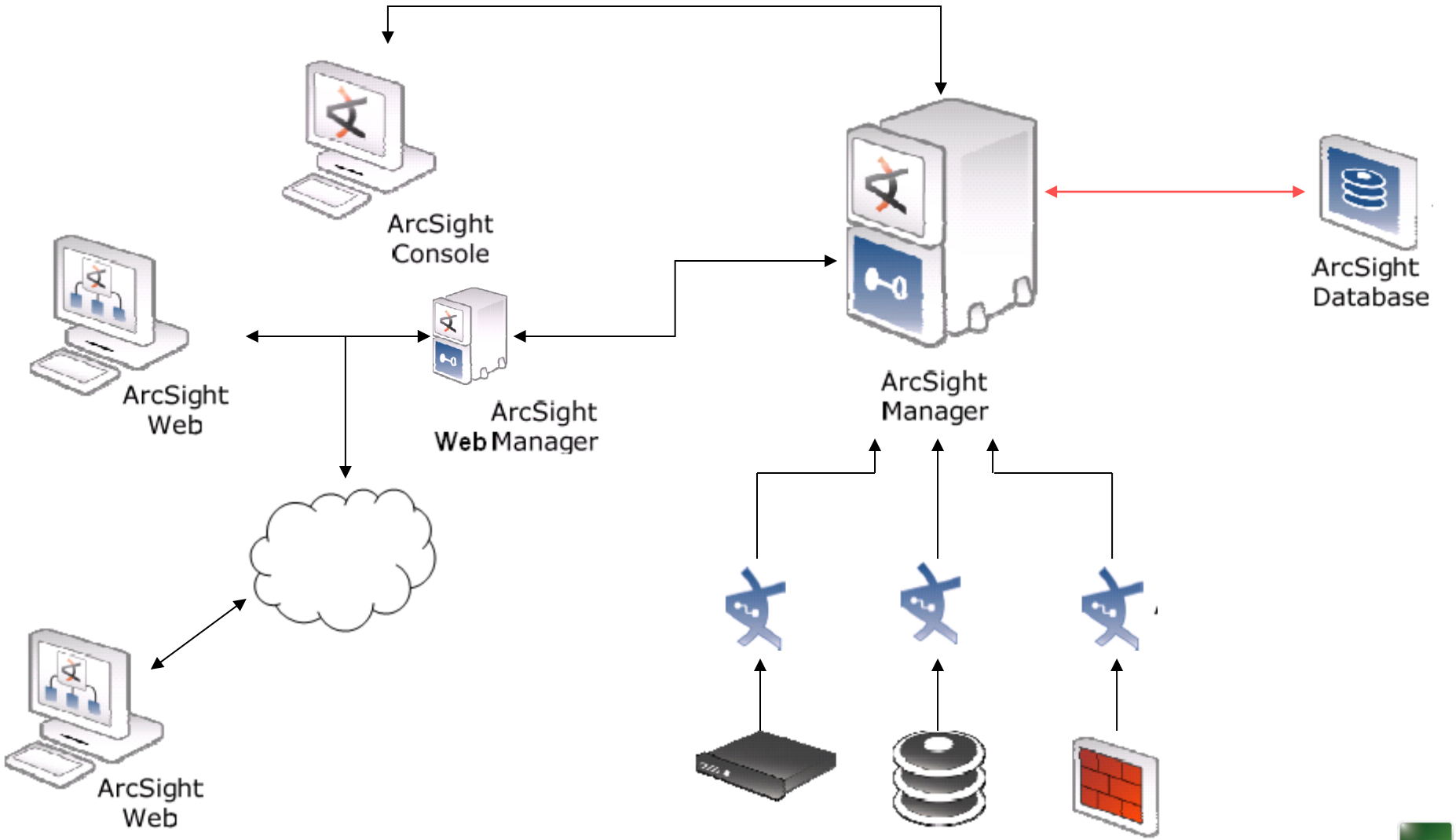
HPE ArcSight ESM поставляется в виде программного решения.

- ESM5 - Лицензируется из расчета 1 лицензия на 1 ядро центрального процессора сервера
- ESM6 – Лицензируется по объему обрабатываемых событий в сутки Гбайт/день

В дополнение к лицензиям HP ArcSight ESM требуется приобрести лицензии и на другие компоненты системы:

- Лицензии HP ArcSight Mon Device и HP ArcSight Mon Desk Device
- Лицензии HP ArcSight Console User и HP ArcSight Web User
- Лицензия HP ArcSight FlexConnect Kit

Схема коммуникации компонентов ArcSight



HPE ArcSight Express:

Поставляется в виде программно-аппаратного комплекса для монтажа в серверную стойку.

Модель	EE7600-250	EE7600-1000	EE7600-2500
Объем событий (поддерживаемых*)	250 EPS	1,000 EPS	2,500 EPS
Дополнительный объем событий (поддерживаемых*)	50 EPS	50 EPS	—
Семейство аппаратных платформ	HP DL380 Gen9 ZE5-2680v3 Kit		
Процессор	Два 12-ядерных процессора Intel Xeon E5-2680v3, 2,5 ГГц		
Размеры (ДхШхВ)	28,75x17,54x3,44		
Память	ОЗУ 6 x 32 Гбайта, 2133 МГц		
Хранение данных	8 дисков по 600 Гбайт (2,4 Тбайт RAID-10)		
Поддерживаемые ОС	Red Hat Enterprise Linux 7.1, 64-разрядная		
Управление	We браузер, CLI, Web-сервисы API		
Интерфейсы Ethernet	4 x 10/100/1000		
Корпус	2U		
Питание	2 блока питания CS Platinum (800 Вт)		

HPE ArcSight Logger:

Решение для долгосрочного хранения и управления информацией о событиях безопасности.

В программном Logger шаг лицензии составляет 5 Гбайт событий в день.

В ПАК Logger все дисковое пространство становится доступным вне зависимости от того, сколько ежедневных событий предусматривает лицензия.

Количество пользователей системы и устройств, с которых выполняется сбор событий, не ограничено.

HPE ArcSight – Новое Лицензирование:

Security Data Platform = Logger + ArcMC Manager + Connectors

Лицензируется по объёму информации (EPS) собираемых коннекторами до фильтрации и до агрегации.

ESM 6.9 - Лицензируется по объёму отфильтрованных и агрегированных событий, пересылаемых коннекторами в сторону продукта.

При покупке нового ESM необходима покупка SDP.

Предлагаемые модели: 250 EPS/ 1000 EPS/ 2500 EPS/ 5000EPS/ 10000 EPS.

Максимум: 23 000 EPS и/или 12 TB хранения.

Миграция 1 Gb/day = 20 EPS.

Сертификация ФСТЭК:

Платформа HPE ArcSight ESM версии 5 и версии 6 от компании Hewlett Packard Enterprise (HPE) прошла сертификацию ФСТЭК. Заявителем проведения сертификационных испытаний программного продукта выступил официальный дистрибьютор решений HPE Security, компания IT Guard.

Сертификат ФСТЭК свидетельствует о том, что программное средство мониторинга результатов регистрации событий безопасности и реагирования на них соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля и технических условий АГРД.509001-03 ТУ при выполнении ограничений по применению, указанных в формуляре АГРД.509001-03 ФО.