10 YEARS JETSECURITY CONFERENCE 2019

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ BIG DATA

Андрей Черных

Руководитель группы внедрения систем мониторинга и защиты приложений
achernikh@jet.su

ЧТО ТАКОЕ BIG DATA?

Big Data – большой объем разнообразных данных с высокой скоростью передачи, требующих экономически эффективных, инновационных форм обработки, обеспечивающих более глубокое понимание, принятие решений и автоматизацию процессов.

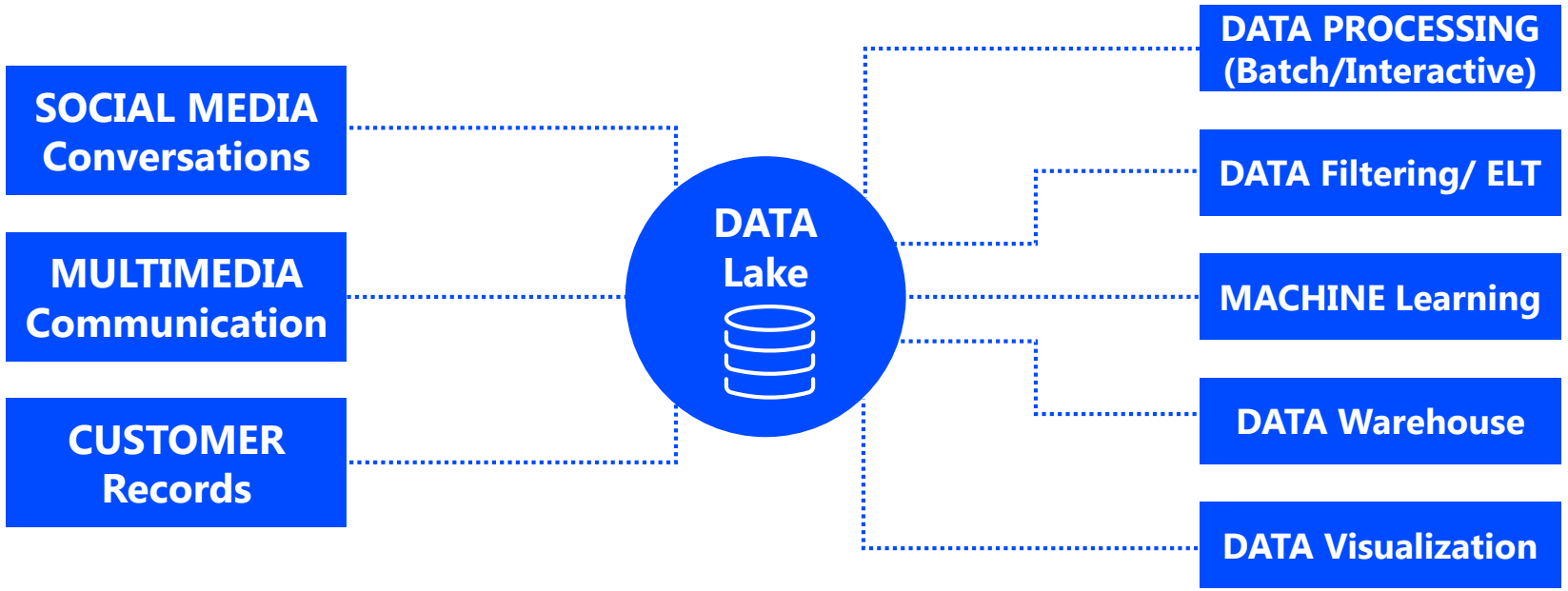
Gartner

Volume	Объем
Velocity	Скорость
Variety	Разнообразие

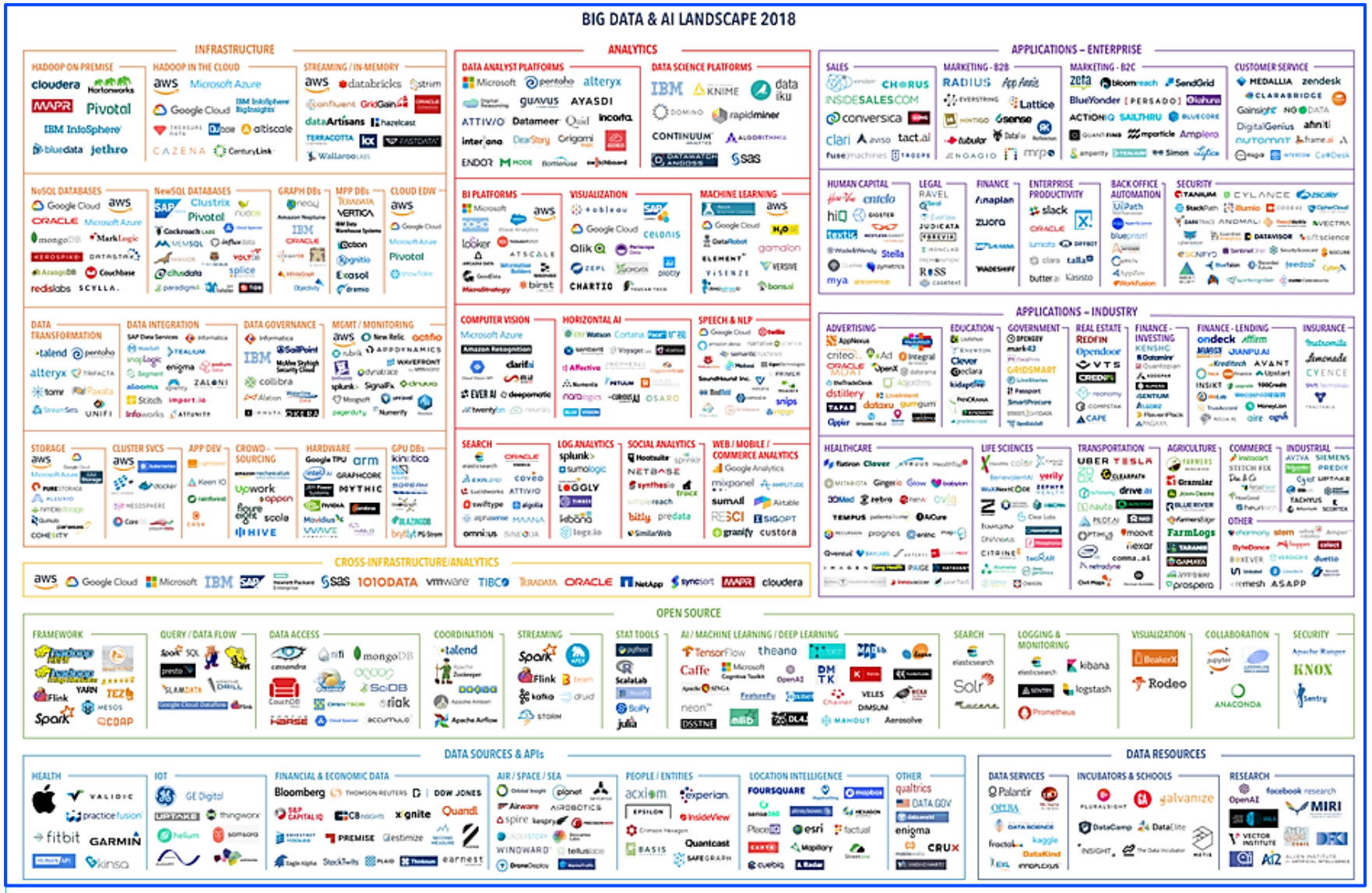
ЧТО ТАКОЕ DATA LAKE?

Data Lake – концепция, при которой в единое хранилище собираются разно-форматные данные для последующей обработки.

Сначала собираем, потом думаем, что с этим делать.

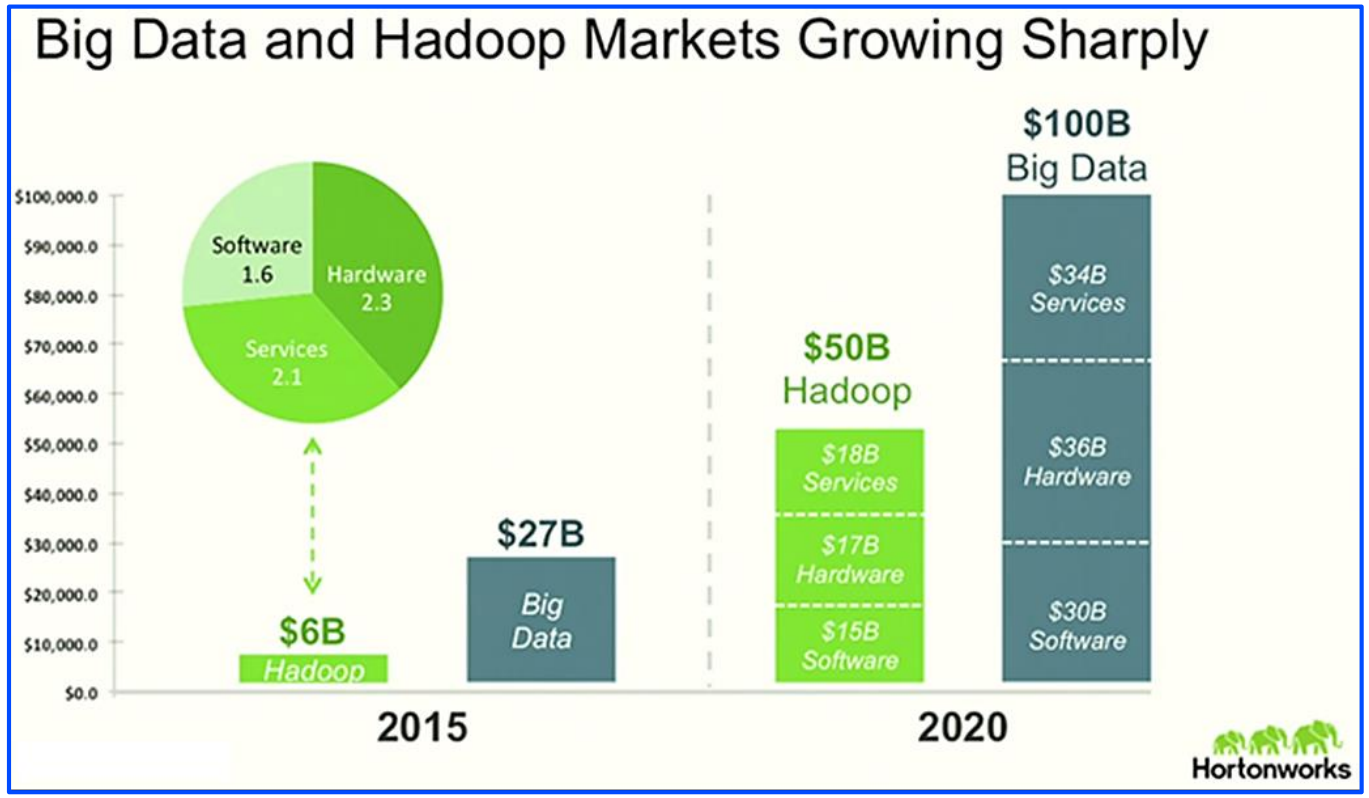


ПЛАТФОРМЫ BIG DATA

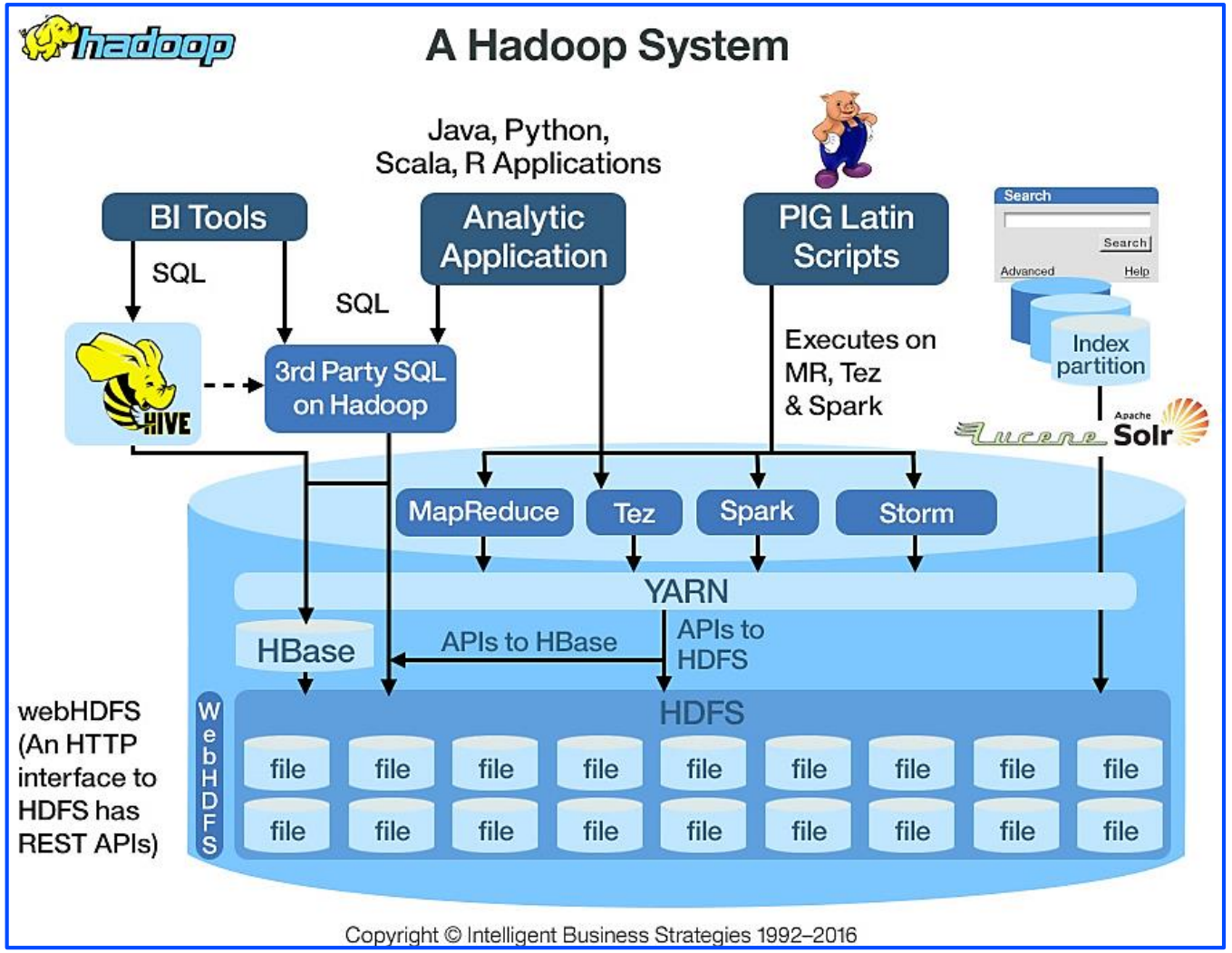


HADOOP

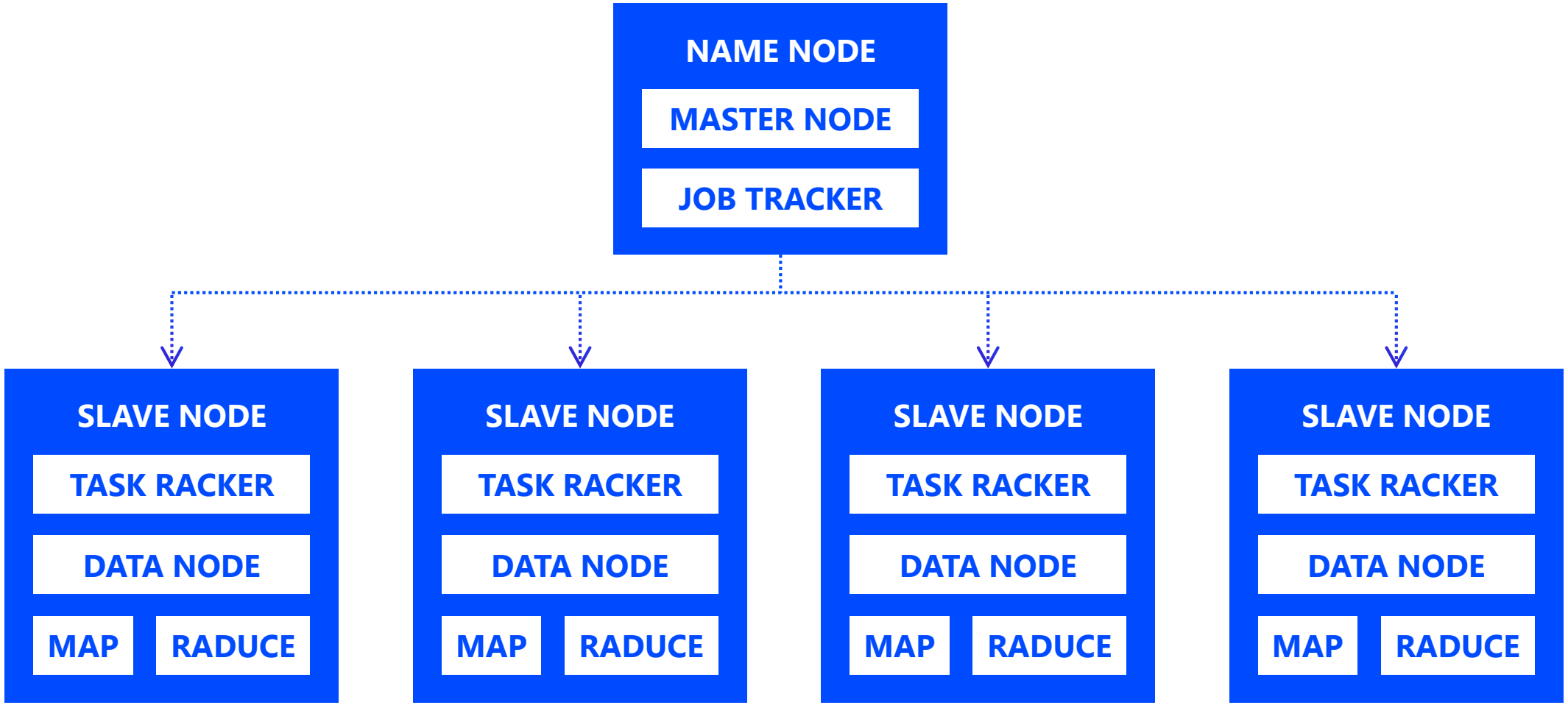
Набор OpenSource программ для распределенного хранения и обработки данных



АРХИТЕКТУРА HADOOP: ПРИЛОЖЕНИЯ



АРХИТЕКТУРА HADOOP: НОДЫ



ВЕНДОРЫ #HADOOP ARENADATA HADOOP

CLOUDERA

HORTONWORKS®

MAPR®

ТОП-3 вендора занимают 56% мирового рынка на 2016. В 2018 году Hortonworks и Cloudera объединились

ПРОДУКТЫ CLOUDERA

- **Cloudera Data Platform (CDP®)** – распределенное хранение и обработка данных
- **Cloudera DataFlow (CDF)** – потоковая обработка данных в режиме реального времени
- **Cloudera Cybersecurity Platform (CCP)** – аналитика событий ИБ в режиме реального времени, нормализация, обогащение, поиск аномалий

ЧТО С БЕЗОПАСНОСТЬЮ?

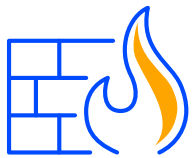
- OpenSource со всеми вытекающими…
- На первом месте функционал, не безопасность
- Многие сервисы без SSL по умолчанию
- Большое количество УЗ «из коробки»
- Разработчики, админы и дата-майнеры с широким набором привилегий

ЧТО С ЭТИМ ДЕЛАТЬ?

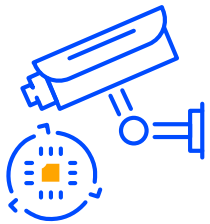
- Поместить систему в закрытый контур
- Пускать пользователей через единый шлюз доступа
- Использовать Kerberos
- Централизованно управлять УЗ
- Контролировать администраторов ОС и Hadoop
- Ограничить доступ к критичным данным
- Сканировать на уязвимости
- Анализировать баги в открытом ПО

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

ЗАЩИТА ИНФОРМАЦИИ



Firewall



Privileged Access Management

Vulnerability scan

ЗАЩИТА ДАННЫХ

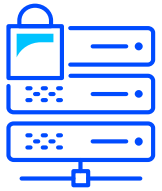
Встроенные средства защиты

Apache Ranger

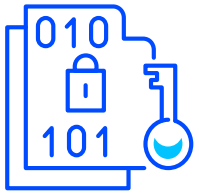
APACHE KNOX

Apache Atlas

Внешние средства защиты



Database Activity Monitoring



Masking/Encrytion/ Tokenization

BIG DATA ДЛЯ БЕЗОПАСНОСТИ

APACHE METRON

ELK Stack

elastic + logstash + kibana

ВСТРОЕННЫЕ СРЕДСТВА ЗАЩИТЫ ДАННЫХ

Apache Ranger – средство разграничения доступа к данным

Apache KNOX – единый шлюз доступа к системе

Apache Atlas – управление метаданными, поиск и классификация данных

APACHE RANGER

ЧТО И КАК ДЕЛАЕТ

- Плагин к приложениям Hadoop
- Регулирует доступ к объектам данных
- Ролевая модель доступа к данным
- Аудит операций пользователей с данными
- Маскирует данные (только Hive)

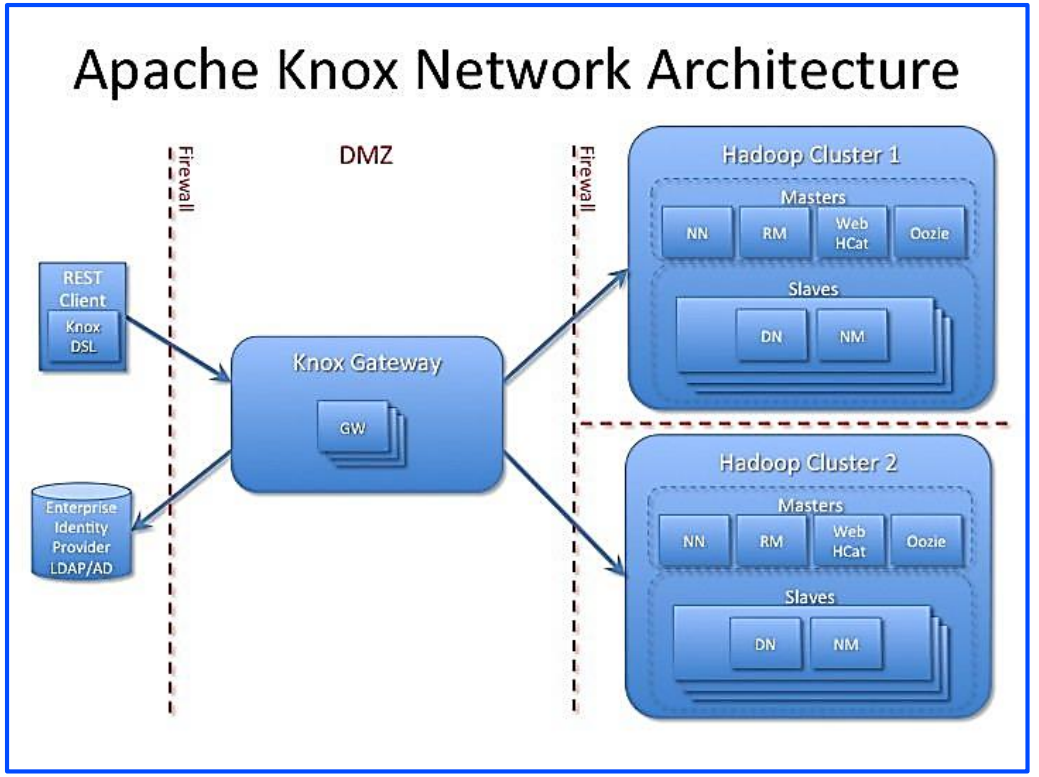
ОСОБЕННОСТИ

- Не контролирует объем возвращаемых данных
- Механизм отчетности не поработан
- Отправка в SIEM и на почту не проработана

APACHE KNOX

ЧТО И КАК ДЕЛАЕТ

- Обеспечивает единую точку доступа
- Проксирует запросы пользователей
- Обеспечивает SSO
- Интегрируется с LDAP и AD



ОСОБЕННОСТИ

- Интеграция с AD пока неполноценная
- Один сервер KNOX —
  до 500 соединений в минуту
- Нужно несколько серверов KNOX
  с внешней балансировкой

APACHE ATLAS

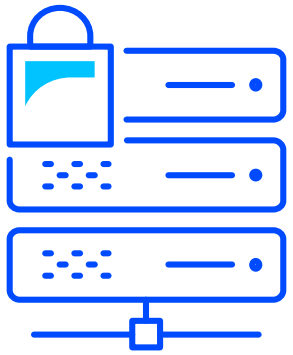
ЧТО И КАК ДЕЛАЕТ

- Хранит метаданные объектов
- Проводит поиск и классификацию
- Отслеживает преемственность
- Вешает тэги на объекты
- Делится данными с Apache Ranger

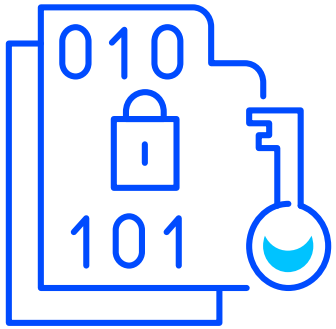
ОСОБЕННОСТИ

- Вспомогательное средство
- Не ищет по содержимому

ВНЕШНИЕ СРЕДСТВА ЗАЩИТЫ ДАННЫХ



Database Activity Monitoring –
аудит и контроль доступа к данным

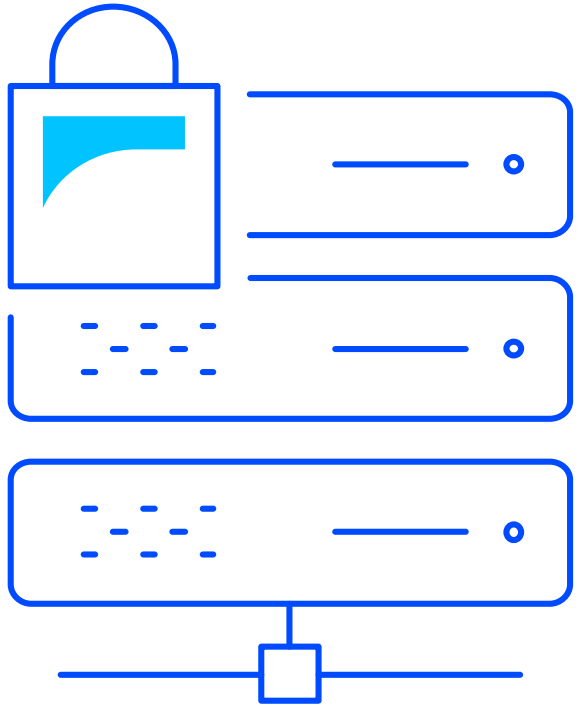


Data Masking/Encryption/Tokenization –
маскирование шифрование
и токенизация данных

DATABASE ACTIVITY MONITORING

ЧТО И КАК ДЕЛАЕТ

- Интегрируется с Ranger
- Агент ставится только на сервер с Ranger
- Работает с данными аудита Apache Ranger
- Классический функционал DAM



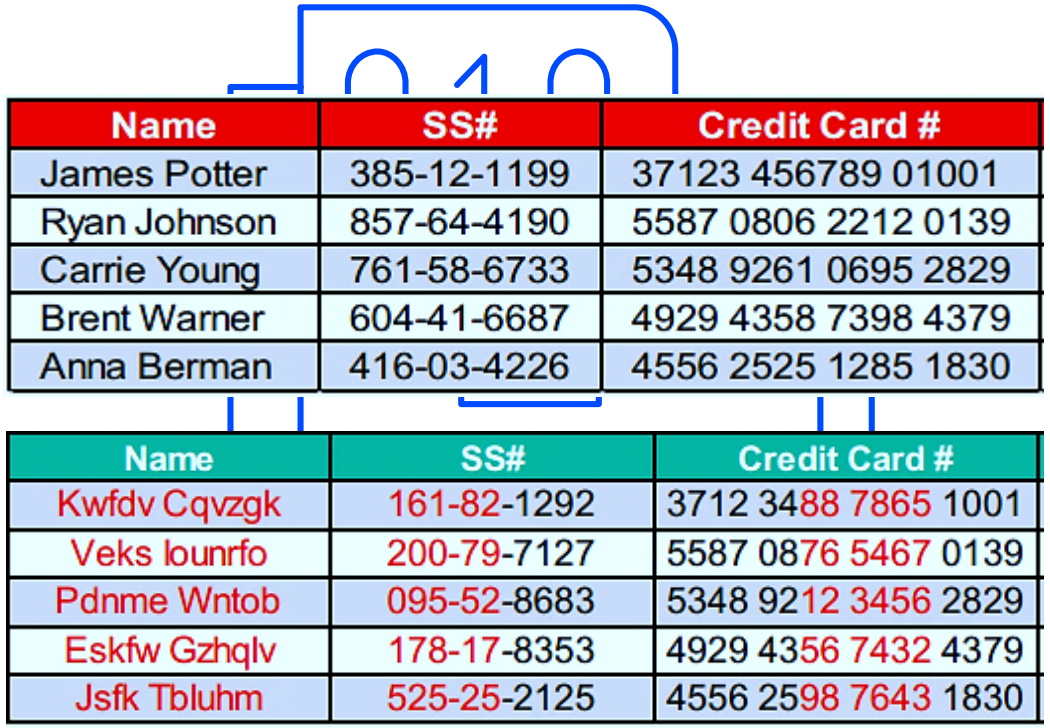
ОСОБЕННОСТИ

- Поддерживает Hive, HBase, HDFS, Knox, Hue, Storm, Kafka
- Требует настройки Apache Ranger
- Те же ограничения, что у Apache Ranger

DATA MASKING/ENCRYPTION/TOKENIZATION

ЧТО И КАК ДЕЛАЕТ

- Шифрование данных с сохранением формата
- Перед укладкой в Hadoop или после
- Агенты ставятся на каждый сервер Hadoop



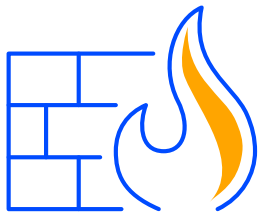
Name	SS#	Credit Card #
James Potter	385-12-1199	37123 456789 01001
Ryan Johnson	857-64-4190	5587 0806 2212 0139
Carrie Young	761-58-6733	5348 9261 0695 2829
Brent Warner	604-41-6687	4929 4358 7398 4379
Anna Berman	416-03-4226	4556 2525 1285 1830

Name	SS#	Credit Card #
Kwfdv Cqvzgk	161-82-1292	3712 3488 7865 1001
Veks lounrfo	200-79-7127	5587 0876 5467 0139
Pdnme Wntob	095-52-8683	5348 9212 3456 2829
Eskfw Gzhqlv	178-17-8353	4929 4356 7432 4379
Jsfk Tbluhm	525-25-2125	4556 2598 7643 1830

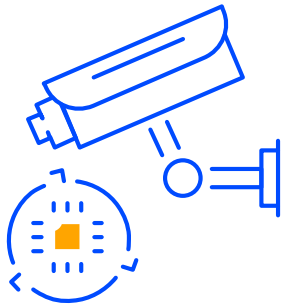
ОСОБЕННОСТИ

- Влияет на исходные данные
- Влияет на обработку данных
- Влияет на производительность

ЗАЩИТА ИНФРАСТРУКТУРЫ



Firewalls – ограничение доступа к сервисам платформы



Privileged Access Management – контроль доступа и мониторинг действий админов на уровне ОС

Vulnerability scanners – сканирование сервисов Hadoop

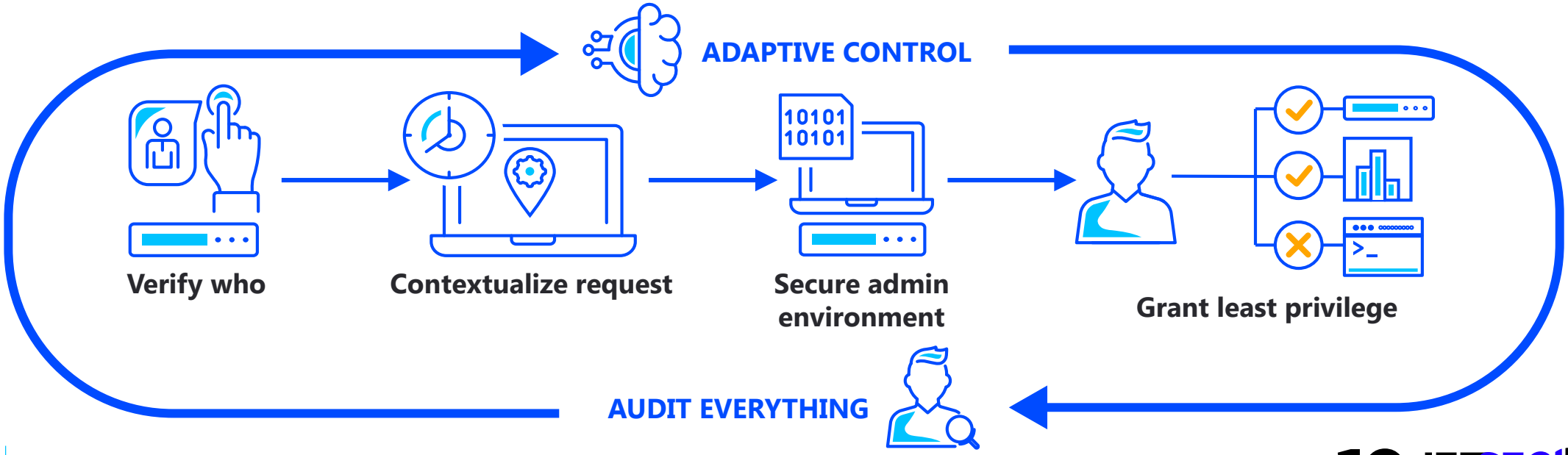
PRIVILEGE ACCESS MANAGEMENT

ДЛЯ ЧЕГО НУЖНО

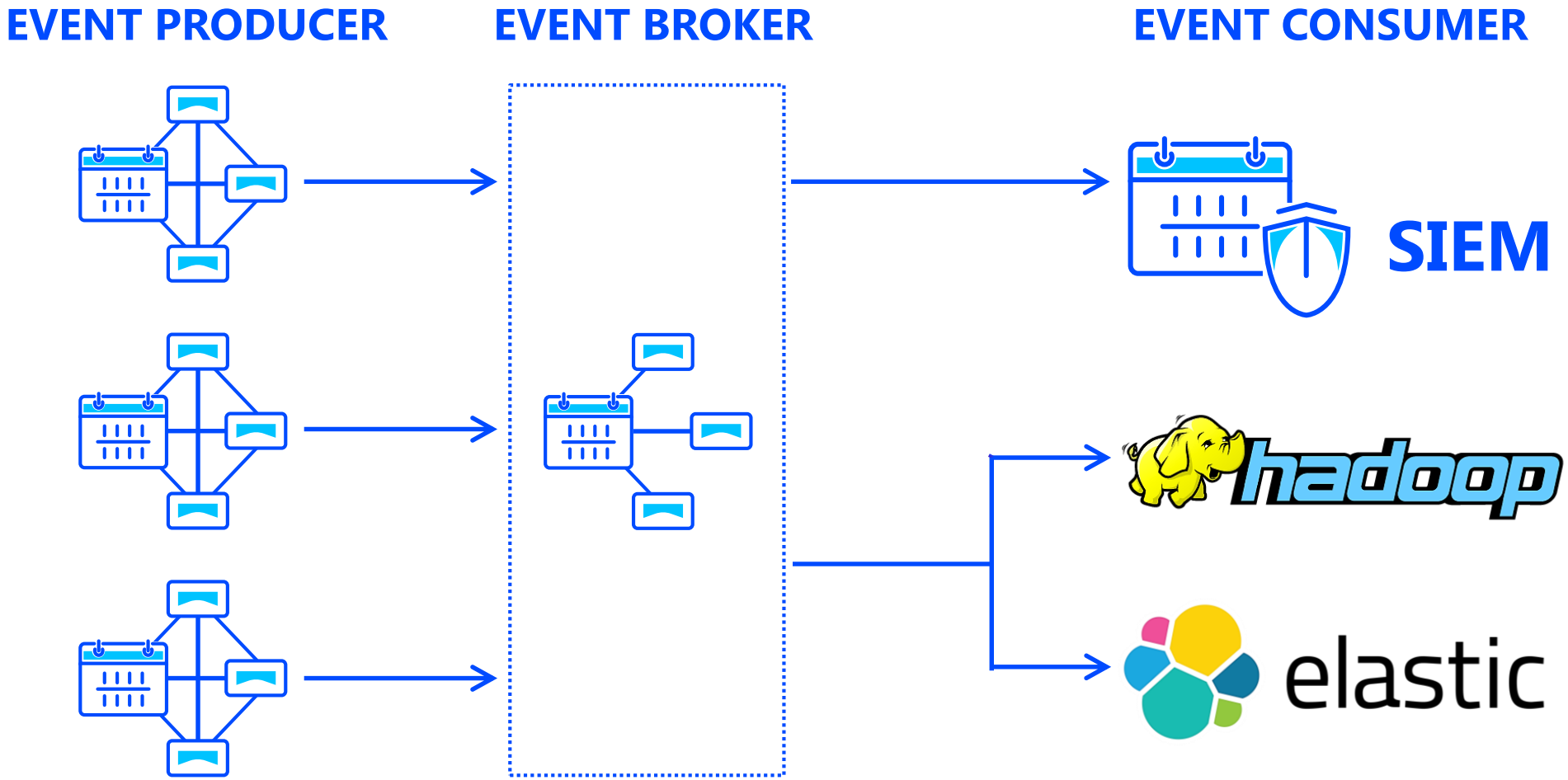
- Централизованное управление УЗ
- Контроль команд
- Аудит действий пользователей (видео/текст)

ОСОБЕННОСТИ

- Агентское или без-агентское решение
- Полноценная защита только с агентами (контроль команд)



BIG DATA ДЛЯ БЕЗОПАСНОСТИ



BIG DATA ДЛЯ БЕЗОПАСНОСТИ

Hortonworks Cybersecurity Platform (HCP) – он же Apache Metron

ElasticSearch Logstash Kibana (ELK)
Для больших объемов данных

Особенности:

- Близки к классу решений SIEM
- OpenSource решения
- Большое хранилище

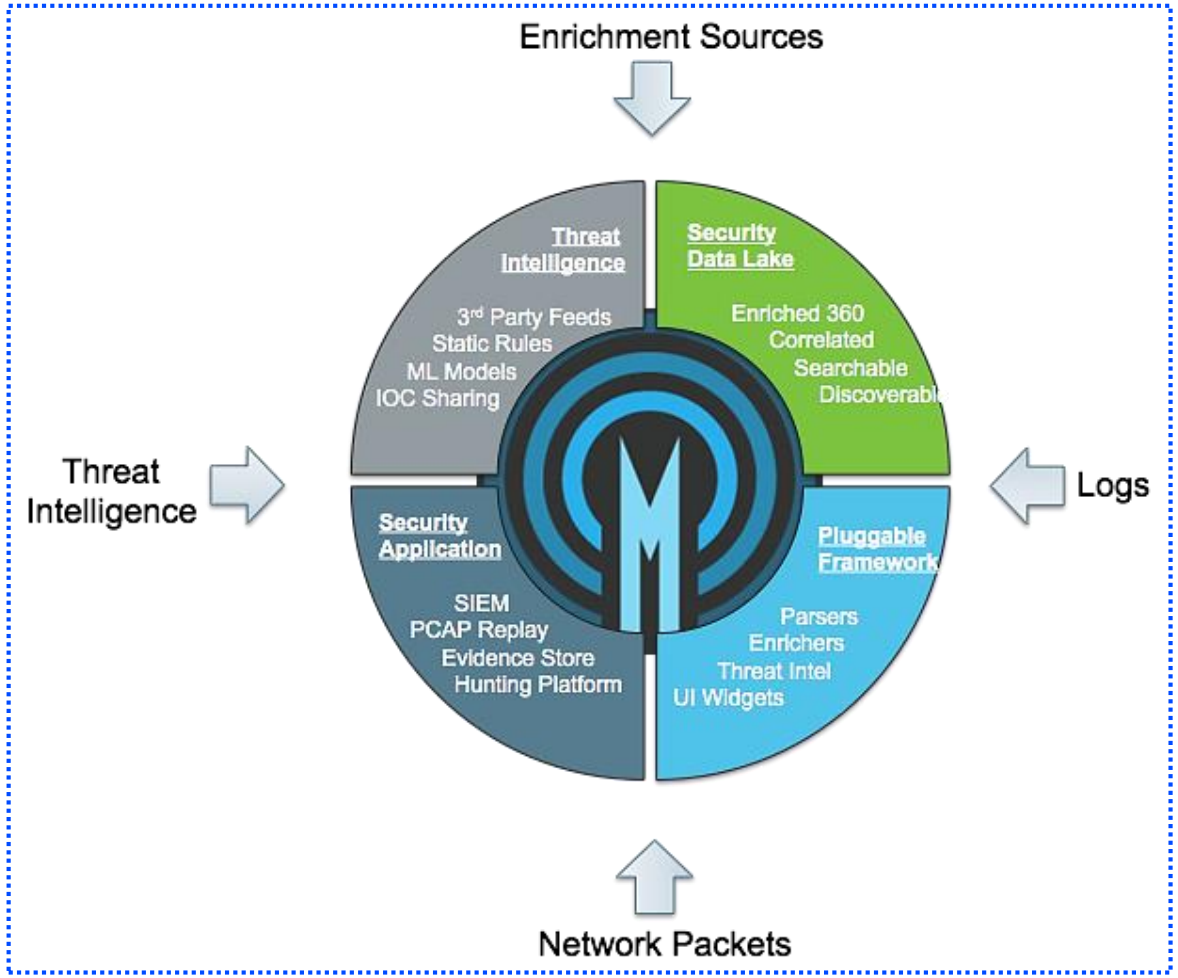
CLOUDERA CYBERSECURITY PLATFORM(CCP)

ЧТО И КАК ДЕЛАЕТ

- Анализирует события real-time
- Обогащает события
- Строит модель поведения
- Детектирует аномалии

ОСОБЕННОСТИ

- Нет в привычном виде правил корреляции
- Правила пишутся на языке Stellar



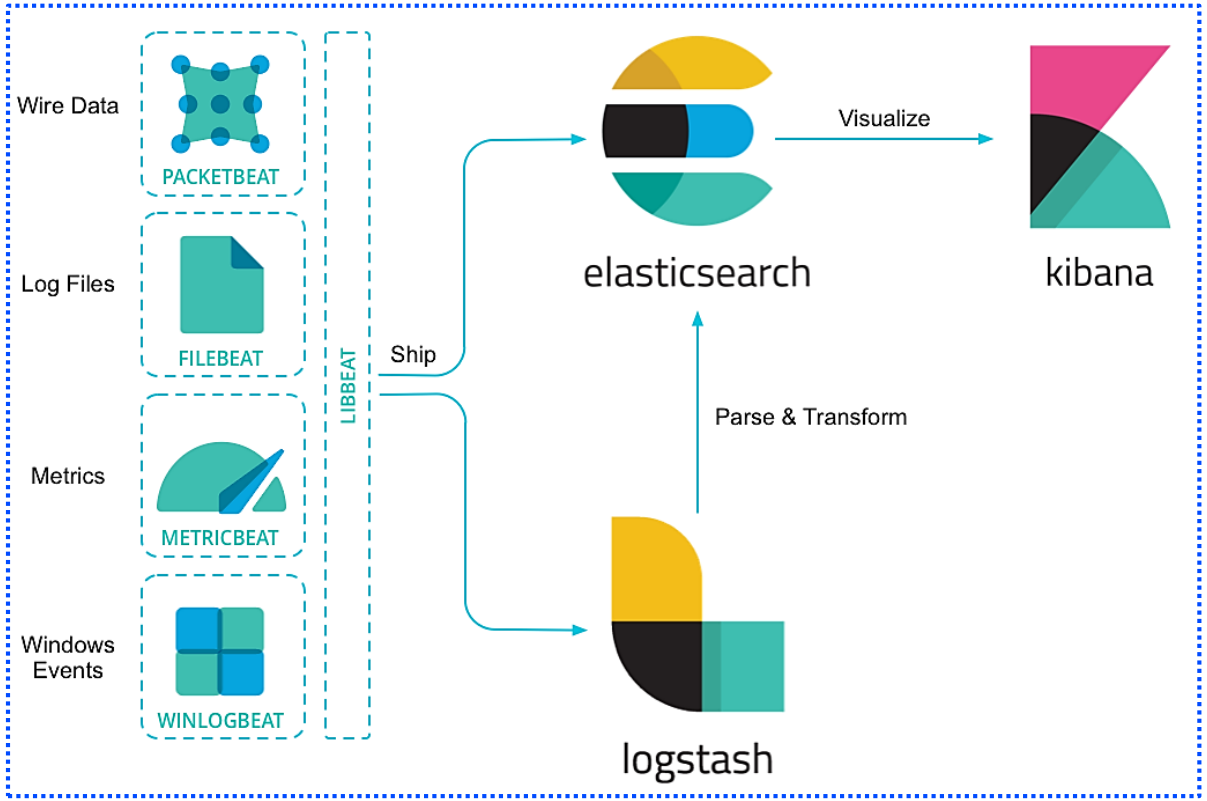
ELASTICSEARCH LOGSTASH KIBANA(ELK)

ЧТО И КАК ДЕЛАЕТ

- Log Management
- Непотоковый анализ событий
- Правила – запросы
- Машинное обучение

ОСОБЕННОСТИ

- Расширенный функционал за $
- Быстрый поиск



10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Андрей Черных

Руководитель группы внедрения систем мониторинга и защиты приложений
achernikh@jet.su