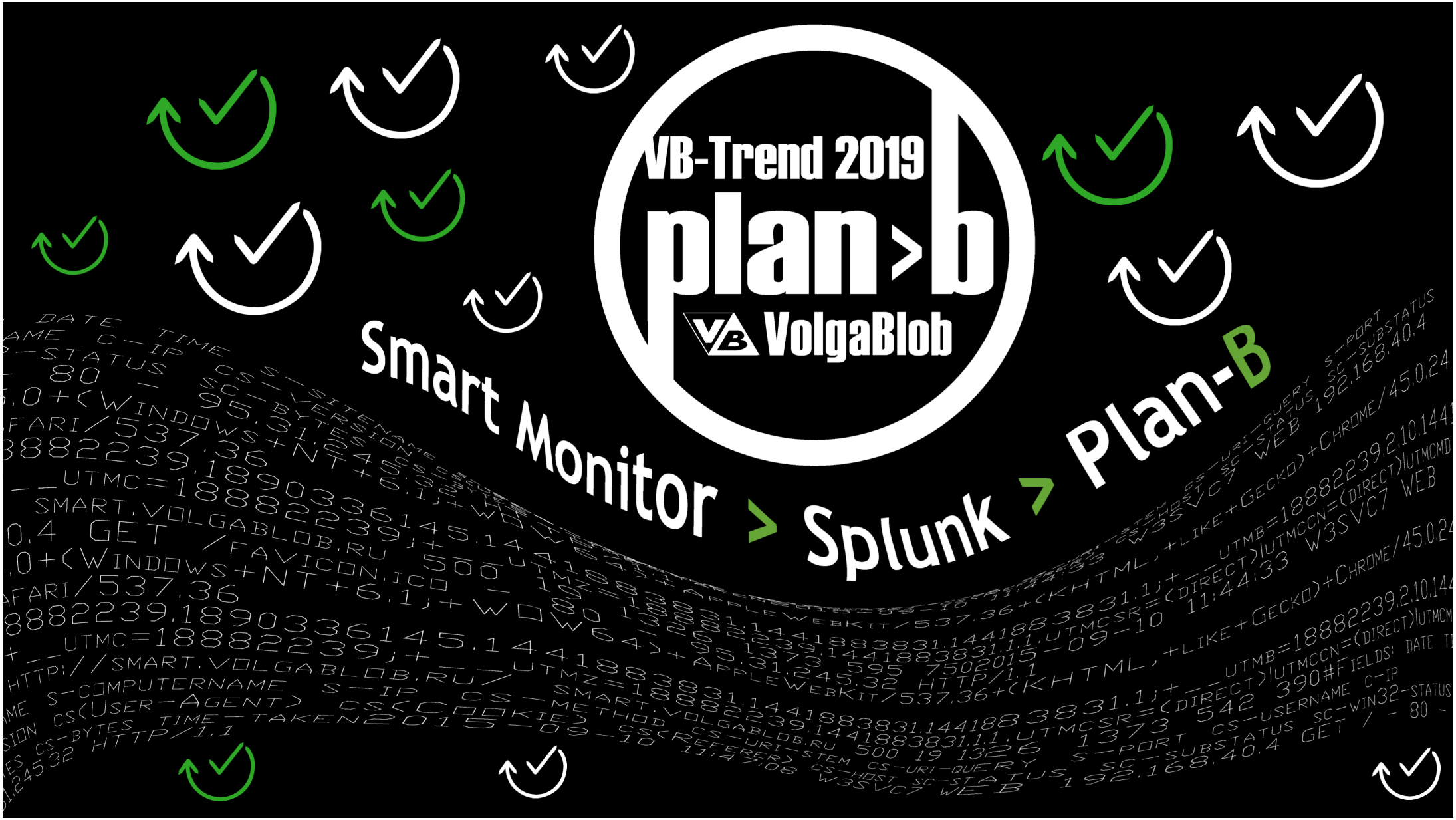
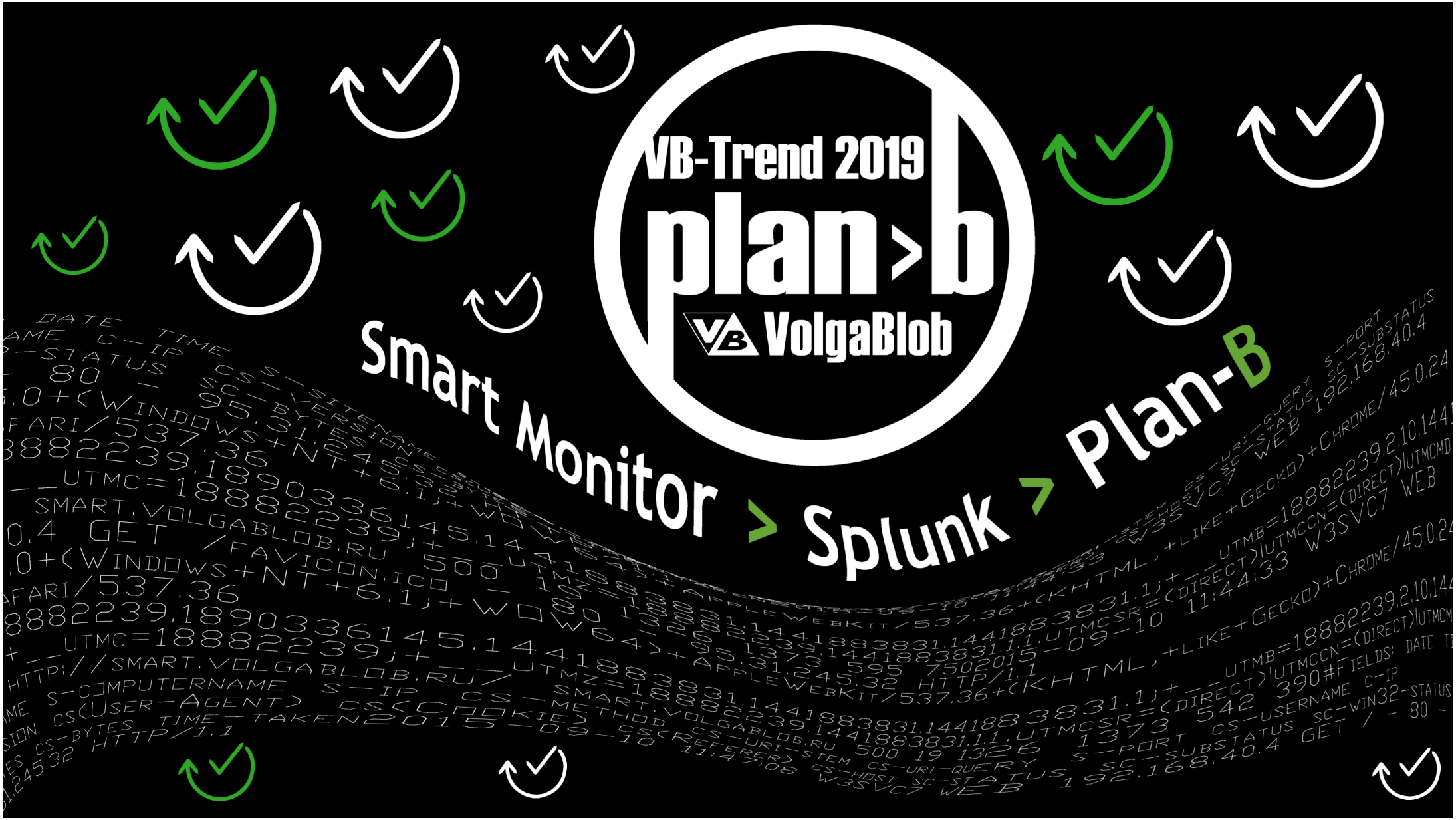

VB-Trend 2019
plan>b
VolgaBlob
Smart Monitor > Splunk > Plan-B

Smart Monitor

Splunk>

>_


VB-Trend 2019
plan>b
VolgaBlob
Smart Monitor > Splunk > Plan-B

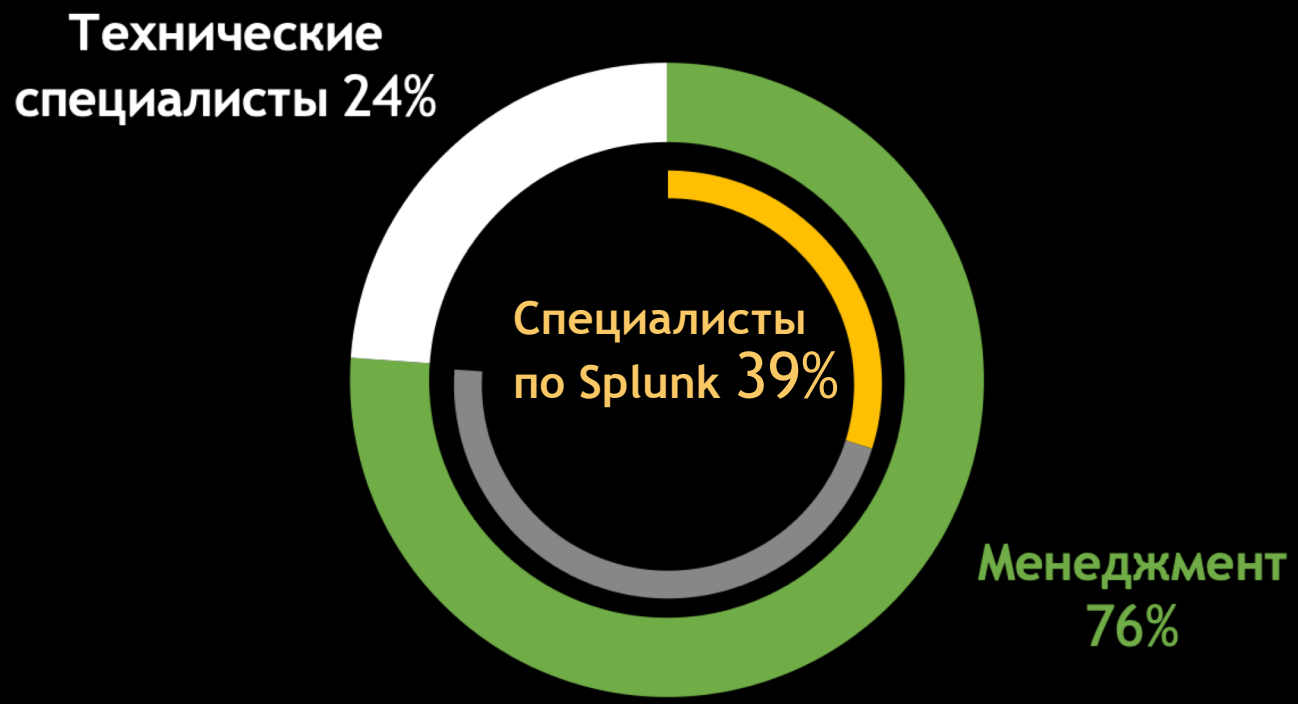
on-line
регистрация

программа
конференции

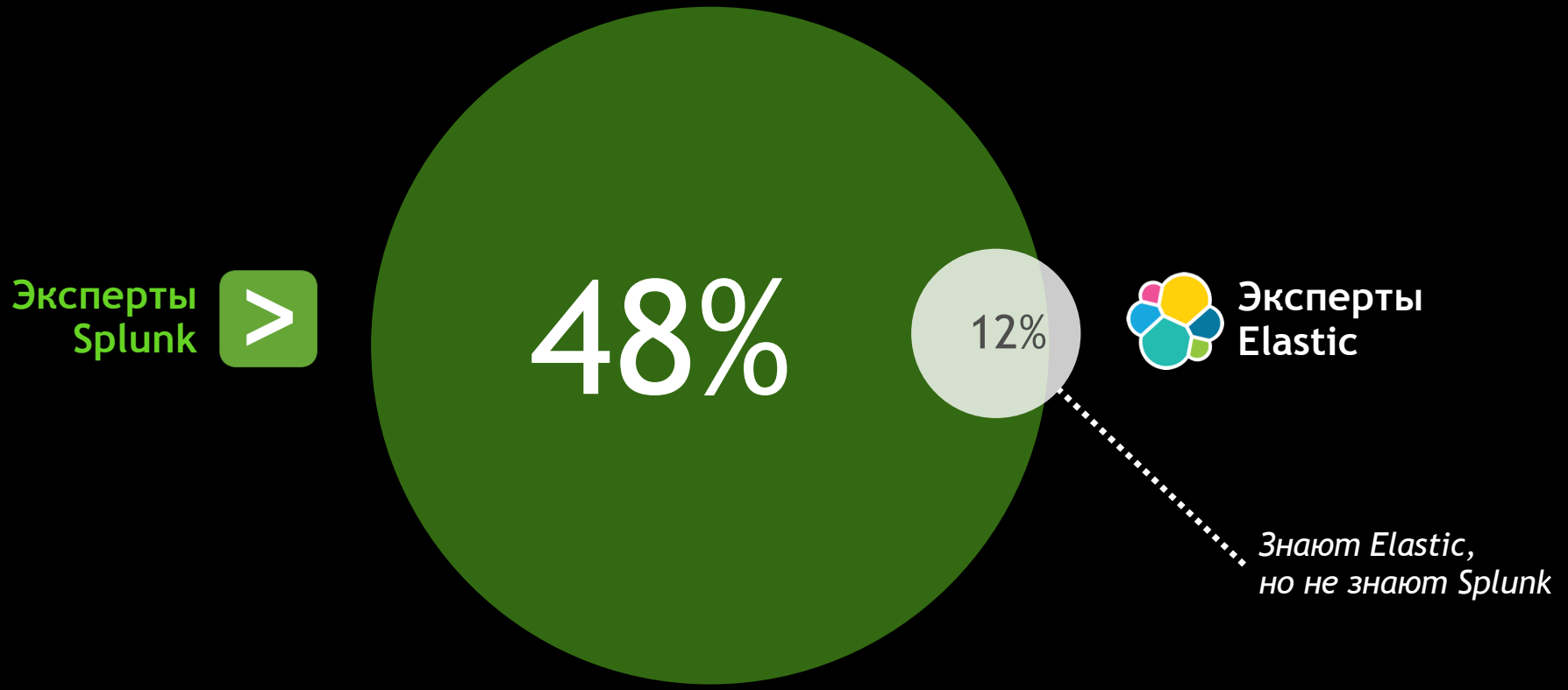
VB-Trend 2019
plan>b
VolgaBlob

SSID: vbtrend
Password: vbtrend2019
Делитесь впечатлениями: #vbtrend

Экспертный клуб VB-Trend 2019



Экспертный клуб VB-Trend 2019



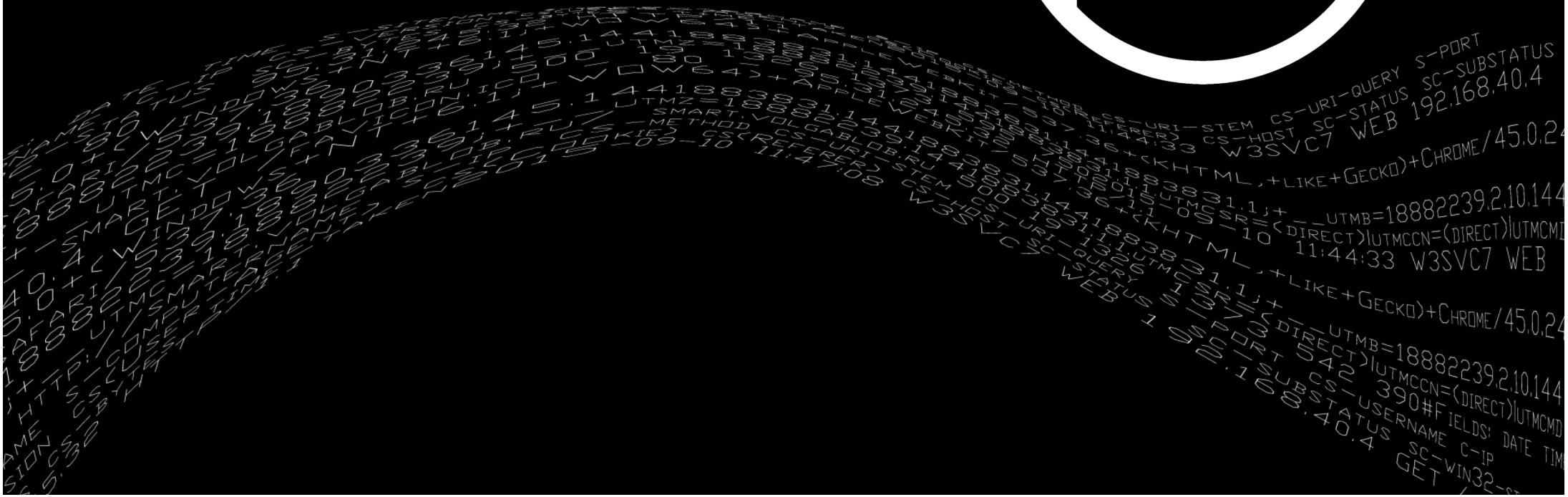
Экспертный клуб VB-Trend 2019

История развития продукта

VB-Trend 2019

plan>b

VolgaBlob



История развития Smart Monitor

2020
Развитие модулей на Splunk и Open Source

2019
30+ проектов на SM

2018
Smart Monitor Splunk App v2.0

2016
Smart Monitor Splunk App v1.0

2014
Заключение партнерства со Splunk. Разработка концепции продукта SM

2013
Выбор платформы SIEM в продуктовый портфель VB

2004-2008
Центр разработки средств криптографической защиты

Определяющий февраль 2019

EMBARGO

splunk>

Plan B

VB-Trend 2019

plan>b

VolgaBlob

Реакция российского рынка

Мнение клиентов Splunk

Наблюдение: ***Россия не любит санкции***

Smart Monitor

Splunk>

>_

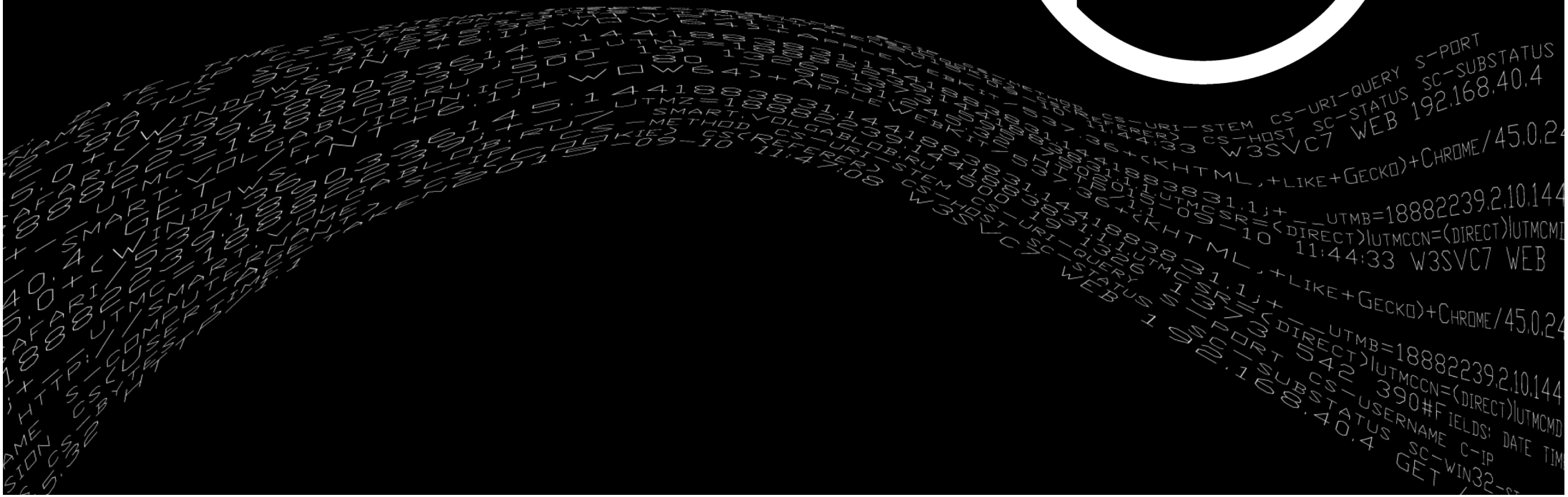
Назначение и сценарии применения

Что поменялось для пользователей?

VB-Trend 2019

plan>b

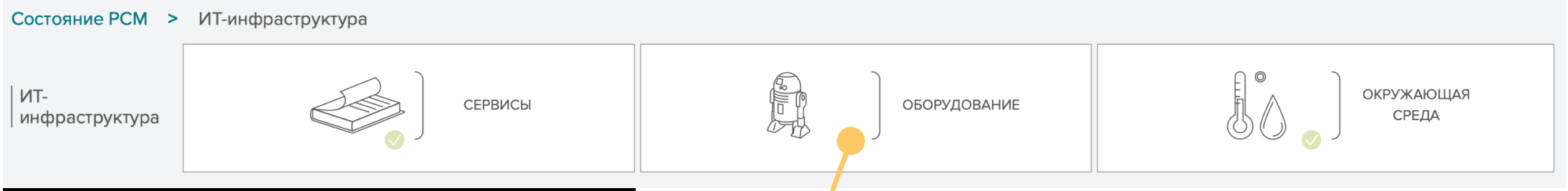
VolgaBlob



Назначение продукта

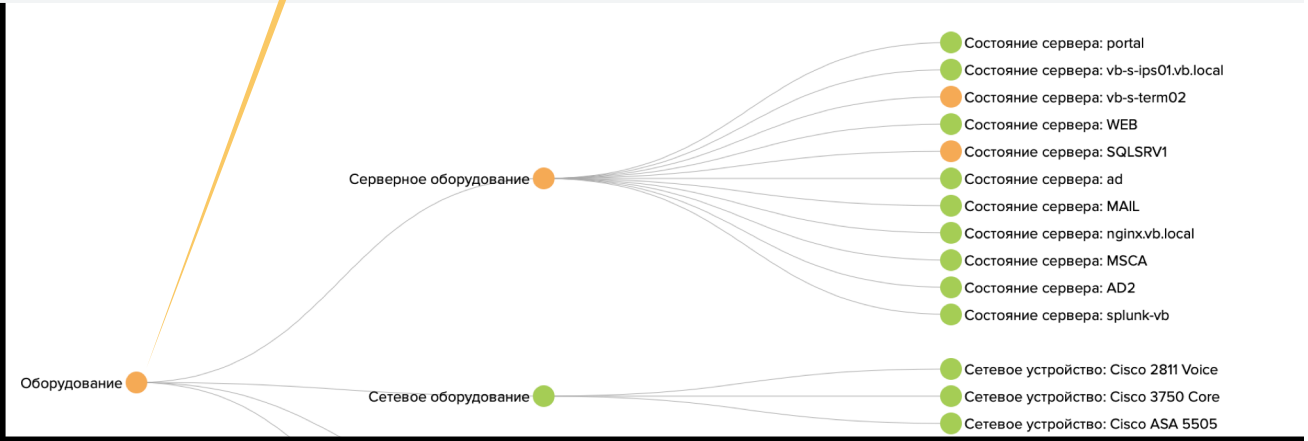
Просто о сложном

Лаконичный универсальный интерфейс оперативного мониторинга: от состояния бизнеса до диагностики принтера



Единая консоль мониторинга для:

- Диагностики инфраструктуры и бизнес-процессов
- Визуального конструктора метрик мониторинга
- Управления инцидентами и активной реакции
- Панелей мониторинга от всего оборудования
- Бизнес-отчетов о real-time статусе систем



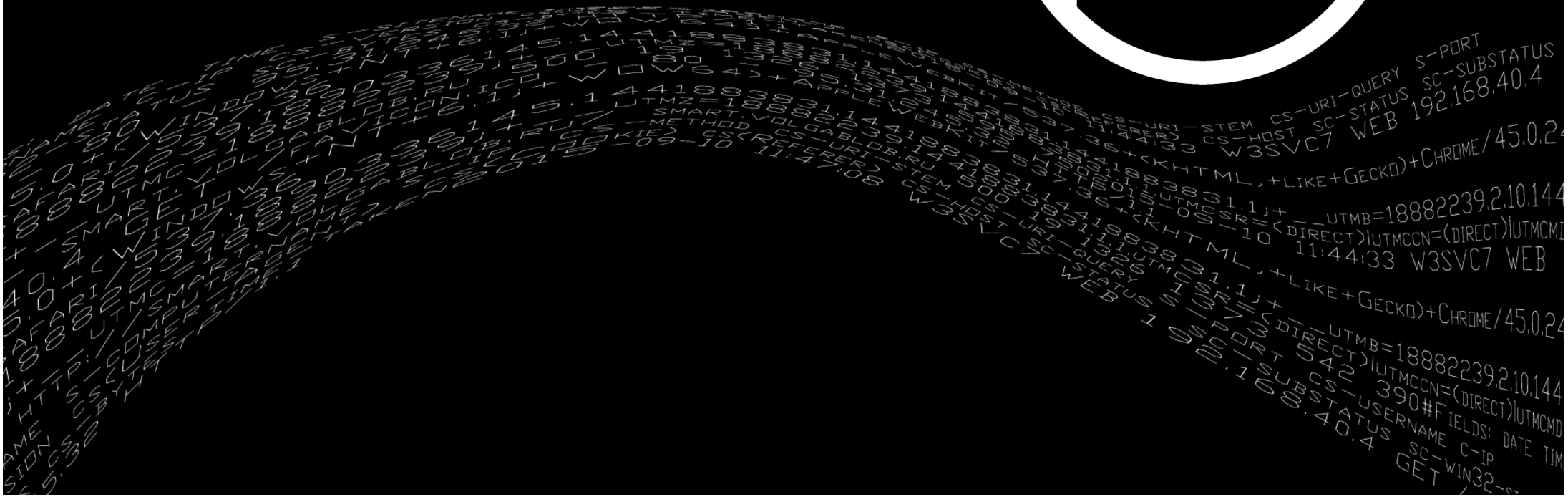
Архитектура решения

Smart Monitor Open Source

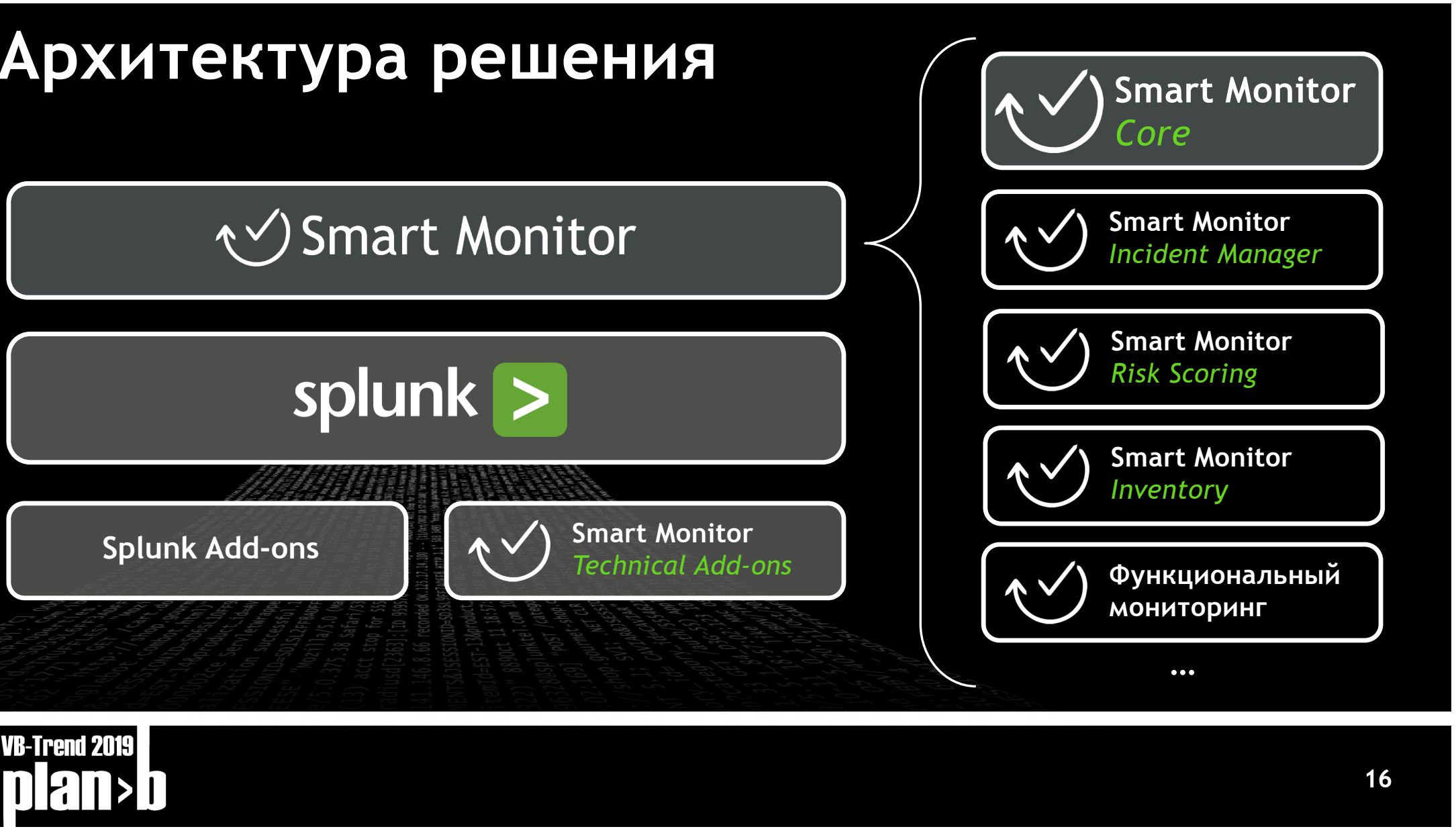
VB-Trend 2019

plan>b

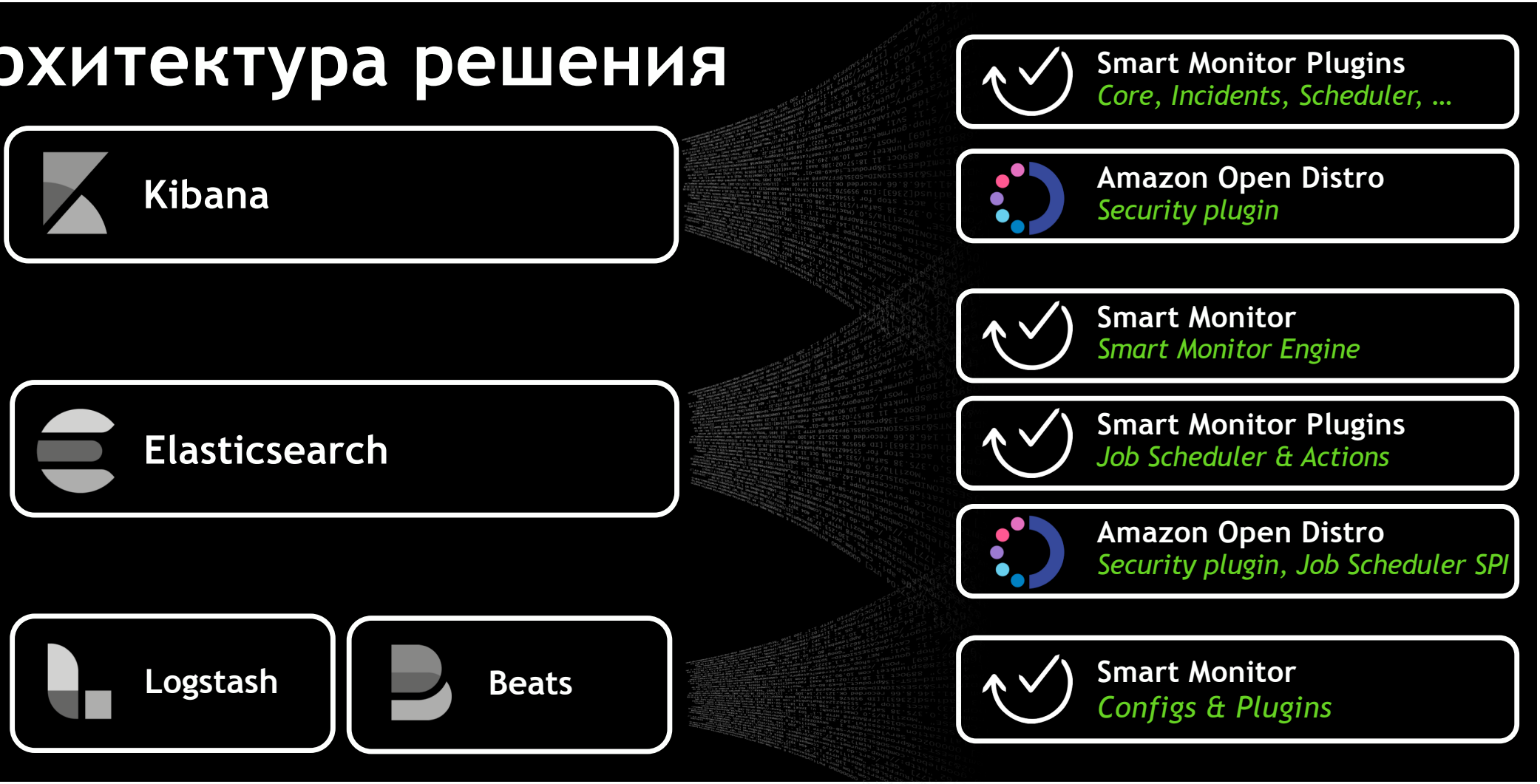
VolgaBlob



Архитектура решения



Архитектура решения



Опрос

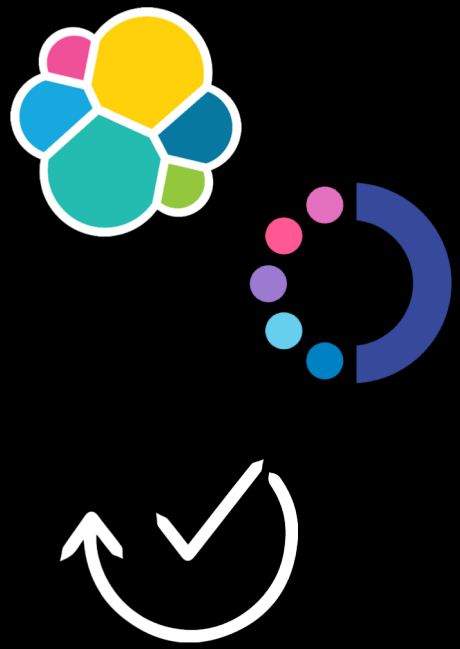
VB-Trend 2019 plan>b VolgaBlob

Каков ключевой *технический* недостаток Elastic Stack по сравнению со Splunk?

- ❑ Меньше способов подключения источников данных
- ❑ Гораздо слабее возможности языка запросов к данным
- ❑ Ниже скорость поиска по хранимым данным
- ❑ Отсутствие поисков по расписанию и управления ими
- ❑ Свой вариант

Поделитесь мнением, пожалуйста!

Цикл разработки и обновления



- Не делаем fork Elastic Stack
- Используем версию OSS (Apache License 2.0)
- Используем актуальную версию Amazon Open Distro for Elasticsearch
- Расширение функционала за счет plugins Smart Monitor
- Обновляем плагины в соответствии с изменениями в очередной версии

Elastic vs Splunk

VB-Trend 2019 plan>b VolgaBlob

Сбор данных

10 — Агентский и безагентский

7 — Агентский и безагентский

Хранение данных

10 — ”Scheme on the fly”, по умолчанию metadata

6 — Все поля индексируются, «жесткий» mapping

Аналитика

10 — Гибкий язык запросов SPL

3 — Проблемы корреляции, точность статистики

Визуализация

10 — Гибкость (SPL), интерактивность

6 — Ограниченный набор настроек, привязка к мастеру

Splunk vs Elastic vs Smart Monitor

VB-Trend 2019 plan>b VolgaBlob

	Splunk	Elastic	Smart Monitor
Сбор данных	10 Агентский и безагентский	7 Агентский и безагентский	7 Агентский и безагентский
Хранение данных	10 ”Scheme on the fly”, по умолчанию metadata	6 Все поля индексируются, «жесткий» mapping	8 Точная настройка
Аналитика	10 Гибкий язык запросов SPL	3 Проблемы корреляции, точность статистики	7 Smart Monitor Engine
Визуализация	10 Гибкость (SPL), интерактивность	6 Ограниченный набор настроек, привязка к мастеру	8 Собственные визуализации SM

Smart Monitor > Цена

- **Smart Monitor** *Core*
- Функциональный мониторинг
- **Smart Monitor** *Incident Manager*
- **Smart Monitor** *Inventory*
- **Smart Monitor** *Cyber Security*
- **Smart Monitor** *Penetration Testing*
- **Smart Monitor** *Risk Scoring*
- **Smart Monitor** *Net Map*

Стоимость решения зависит от состава и числа модулей

Нет привязки к объему данных

Первые проекты	2019-Q2
Предварительный заказ	2019-Q4
Партнерская программа	2020-Q1
Реестр отечественного ПО	2020-Q2
Сертификация ФСТЭК	2020-Q4

Практические сферы применения

VB-Trend 2019 plan>b VolgaBlob

Smart Monitor

Мониторинг бизнес-процессов

- *Возможности применения мониторинга бизнес-процессов для целей различных бизнес-функций*
- *Путь от SIEM к решению Big Data, полезному бизнесу. Опыт компании СУЭК*

Мониторинг кибербезопасности

- *Smart Code - решение для комплексного мониторинга средств защиты Кода Безопасности*
- *Автоматизация SOC: управление инцидентами. Новые возможности Smart Monitor*

Мониторинг ИТ-инфраструктуры

- *Мониторинг сред контейнеризации на примере Kubernetes и Docker*
- *Новый взгляд на автоматизацию оценки соответствия. Первое российское применения стандарта OSCAL*

Спасибо за внимание!

… какие тут могут быть вопросы? :)

VB-Trend 2019

plan>b

VolgaBlob