FORTINET

Инструменты CISO для управления информационной безопасностью

Дмитрий Купецкий, Fortinet SE

SECURITYDAY

Драйверы развития ИТ инфраструктур и ИБ

Драйверы развития ИБ

Современные тренды – Internet 2 в ближайшее время

Возросшее количество атак

65K инцидентов в отчёте только Verizon DBIR

SDN/NFV

Software-defined everything. SD WAN

Virtualization

80% приложений виртуализированы

SaaS

По статистике около 10 приложений компании размещены в облаке

Mobile

Не внедрён контроль устройств (BYOD)

SSL Traffic Growth

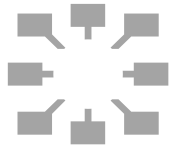
40% всего трафика зашифровано SSL

Social

Рост использования полосы пропускания

IoT

20B устройств подключено к сети



100G

Bandwidth

Wi-Fi достиг скоростей LAN. 100G сети уже построены. Рост бизнес трафика на 20% ежегодно.

Analytics

Big Data

5G

Wireless

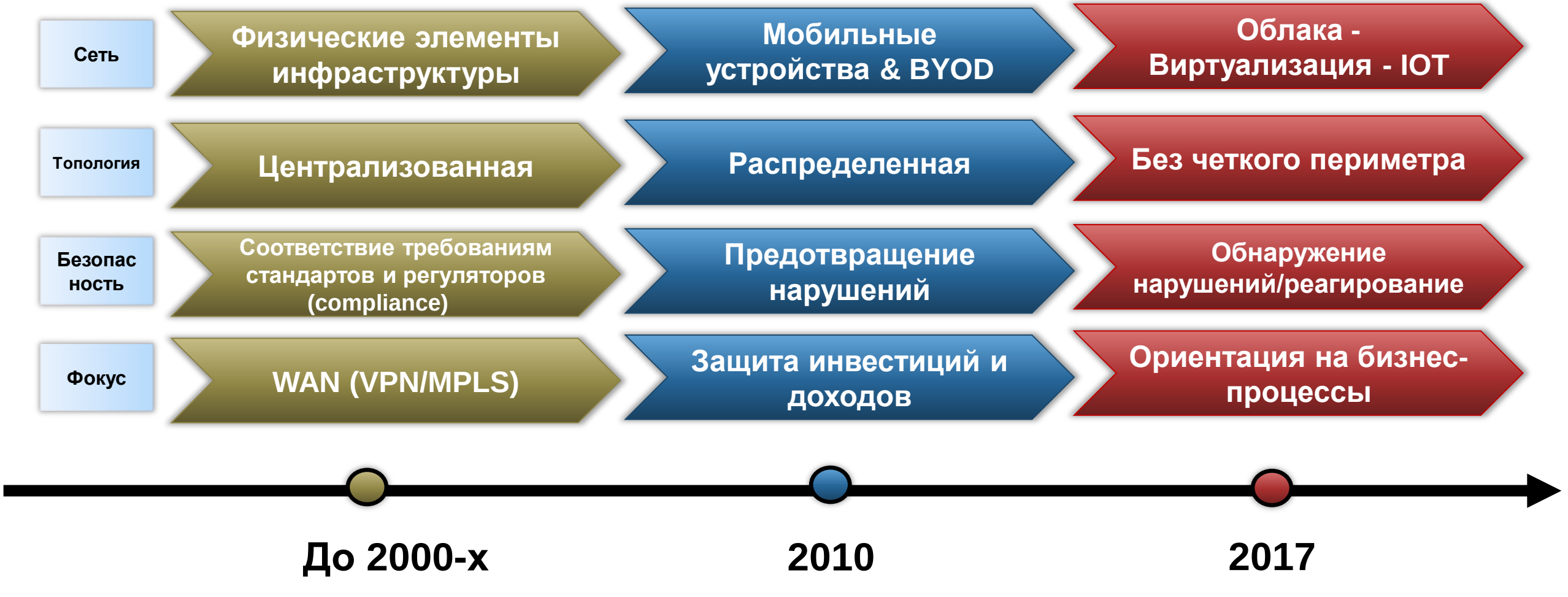
Internet 2

100 Gbps и

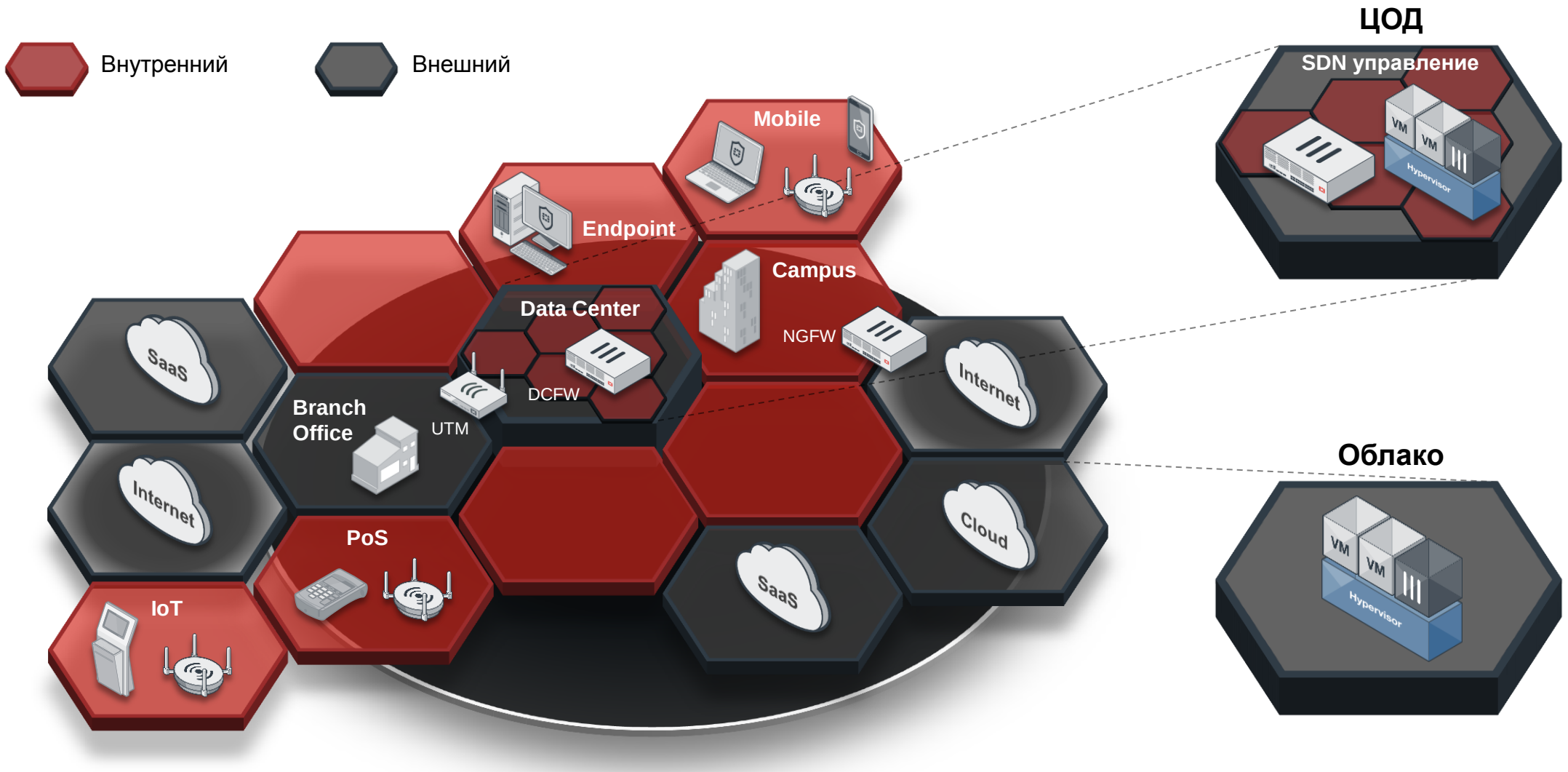
UHDTV

БУДУЩЕЕ

Эволюция сетевой инфраструктуры



Высокий уровень Сегментации



Роль и задачи CISO в современных условиях

FORTINET

Задачи, возлагаемые на CISO

Доступ и авторизация

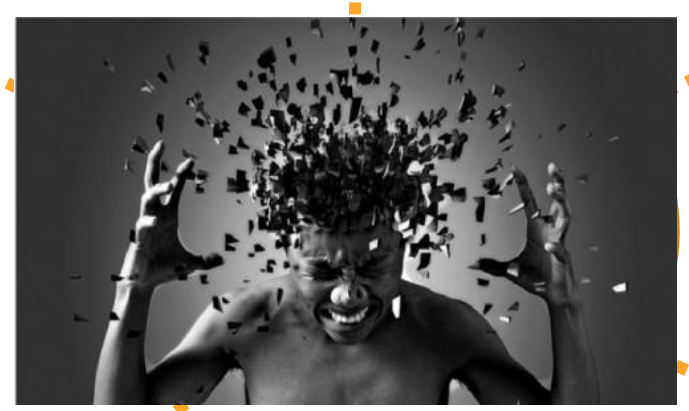
- *Контроль привелегированных акгаунтов?*
- *Доступ только атворизованных пользователей к критическим системам?*
- *Разграничение доступа пользователей?*

СЕТЬ

- *Внедрены ли меры защиты сетевых инфраструктур?*

Приложения

- *Оценка рисков использования внедренных приложений?*
- *Внедрены ли меры защиты приложений?*



Угрозы безопасности

- *Есть ли оценка ущерба и масштабов угроз?*
- *Наличие стратегии и способов противодействия?*

ОБЛАКО

- *Миграция сервисов в облака с точки зрения рисков безопасности?*

Mobile

- *Безопасна ли применяемая инфраструктура и приложения?*

Стабильность бизнеса

- *Есть ли уверенность в стабильности работы бизнеса в кризисных условиях?*

Внешние риски

- *Обеспечивается ли защита данных при взаимодействии с подрядчиками?*

Соответствие

- *Соответствует ли инфраструктура текущим требованиям регуляторов?*
- *Что делается для обеспечения соответствия?*

Роль CISO как руководителя и сотрудника

Экспертиза в области ИБ

- *Актуальные компетенции*
- *Поывшение квалификации*

Консалтинг

- *Обеспечение консультаций бизнеса по актальным вопросам ИБ*

Внедрение ИБ

- *Руководство внедрением новых решений*
- *Обеспечение поддержки уже внедренных решений*

Актуальные тренды

- *Быть в курсе тенденций*
- *Повышать квалификацию*

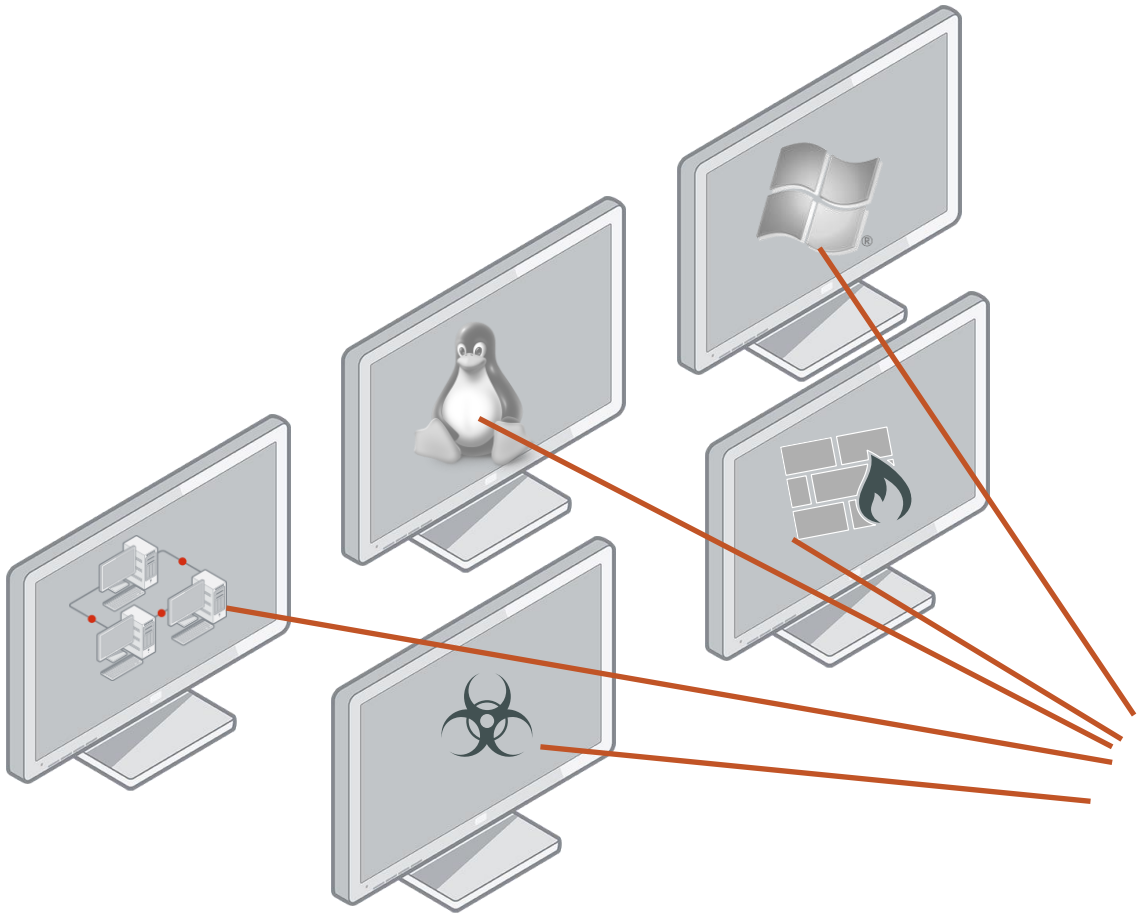
Найм квалифицированного персонала

- *Поиск и найм необходимого состава профессионалов ИБ*

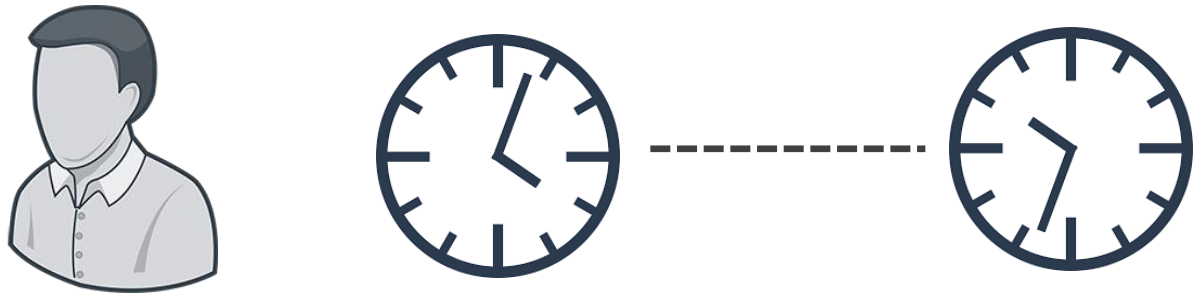
Составление отчетности

- *Месячная/квартальная/годовая отчетность о состоянии ИБ для бизнеса*

Системы мониторинга инфраструктуры плохо масштабируются…



- *Большое количество систем для мониторинга*
- *Необходимо много времени на расследование инцидента.*
- *Обнаруживался ли инцидент ранее?*
- *Системы все еще скомпрометированы или подвержены риску?*
- ***Давайте надеяться, что нет…..***

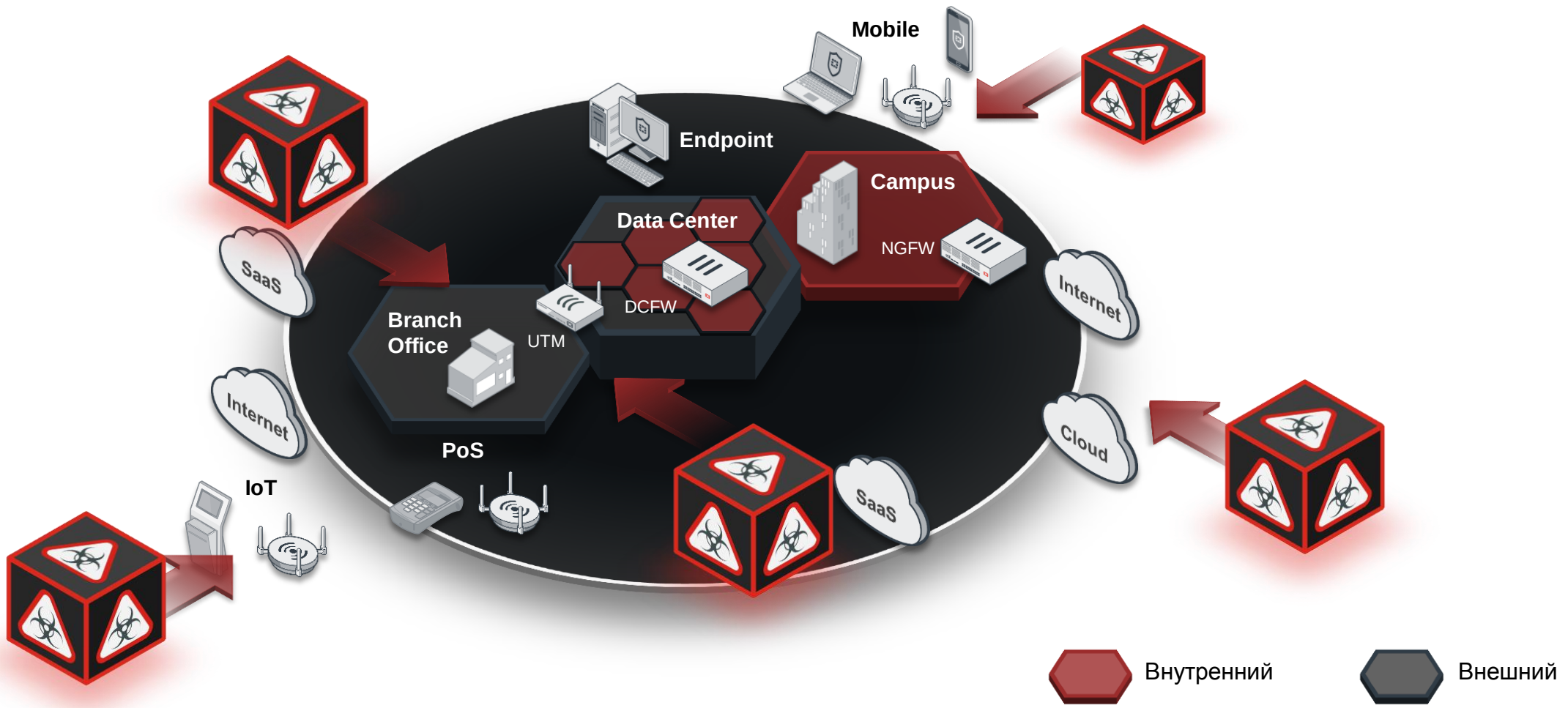


Жизнь была прекрасна

До возникновения первого реального инцидента ИБ…

Мне нужен лог приложения «X» → Лог нужен за последние 4 месяца → В логе нет нужной информации

Площадь атак стремительно растет с высокой динамикой



Динамика развития ситуации

SIEM как средство управления событиями ИБ

FORTINET

Что такое SIEM?

SIM – Security Information Management

- *Сбор*
- *Хранение*
- *Индексация*
- *Исторический поиск*

SEM – Security Event Management

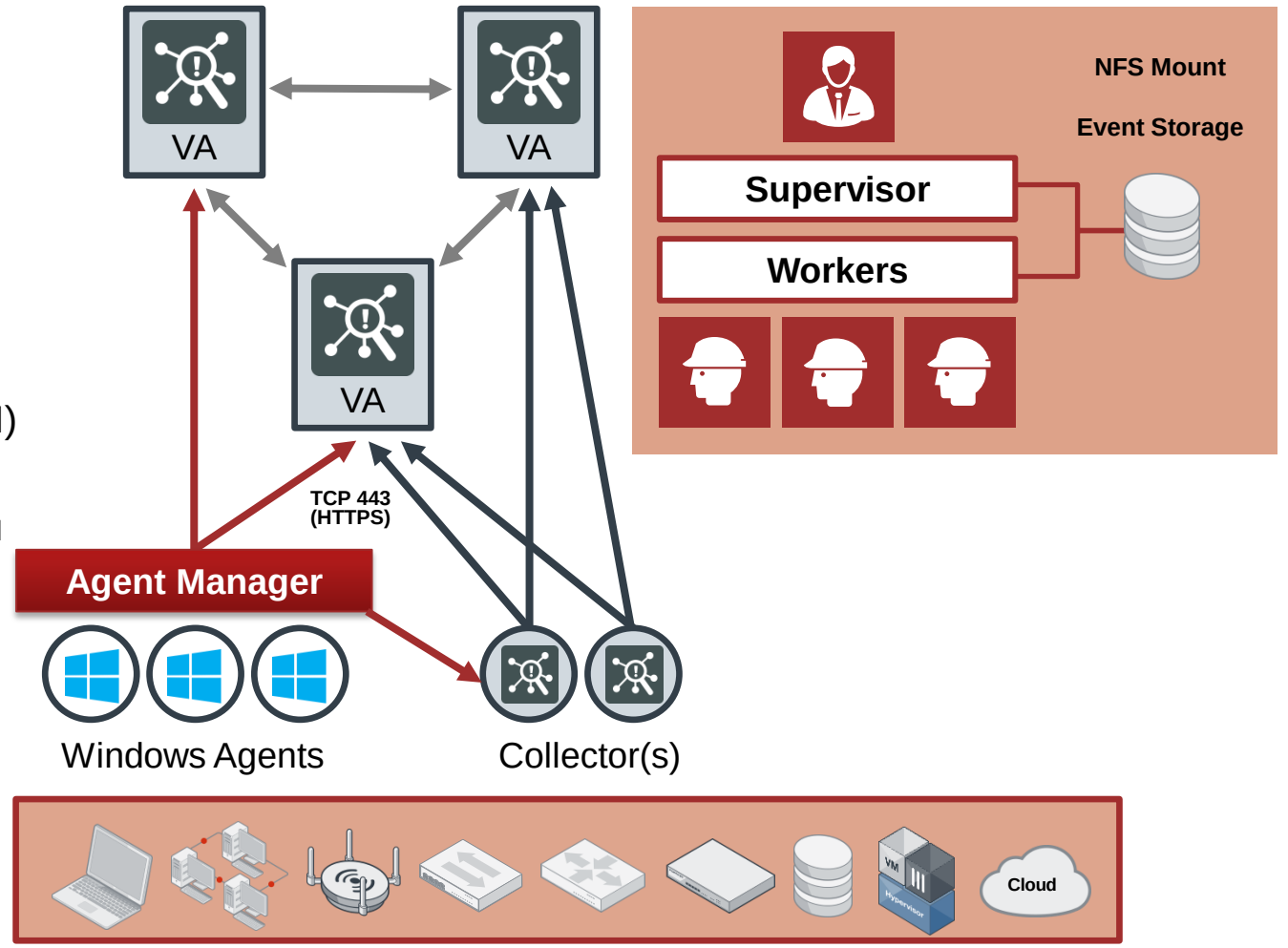
- *Идентификация событий*
- *Корреляция*
- *Отчетность*

Что такое SIEM?

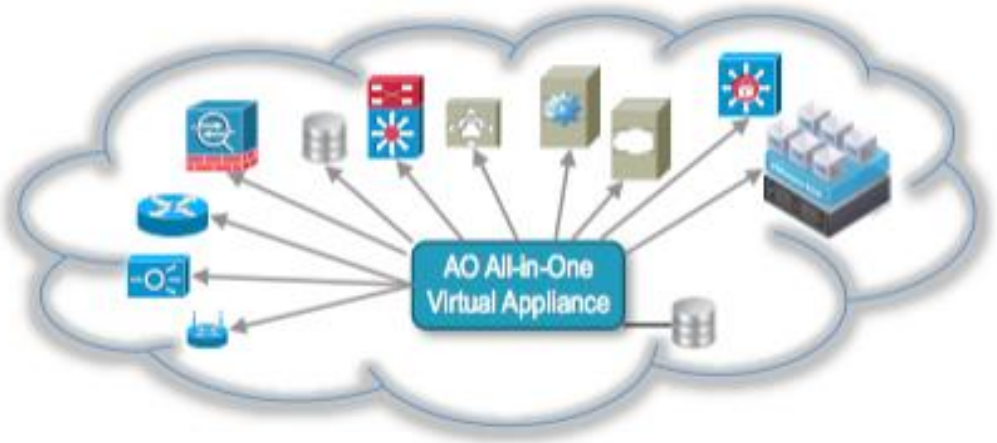
- SIEM - Security Information & Event Management – система управления событиями информационной безопасности
- Ввод - централизованная точка сбора логов всей инфраструктуры
- Обработка – Анализ/корреляция событий
- Вывод – оповещение/отчетность/текущий мониторинг

Иерархическая быстро масштабируемая архитектура

- **Виртуальное/физическое исполнение**
  - » Расположение: Собственная инфраструктура - ЦОД - Облако
- **Архитектурные элементы**
  - » **Супервизор**
    - Основной компонент решения (веб-сервер, сервер приложений, сервер баз данных, GUI)
  - » **Обработчик(и) (Workers)**
    - Аналитика и текущая обработка своей части событий ИБ при подчинении супервизору
  - » **Коллектор(ы)**
    - Сбор и обработка событий в точке установки
  - » **Windows Agent(s) and Manager(s)**
    - Более подробный и точный мониторинг

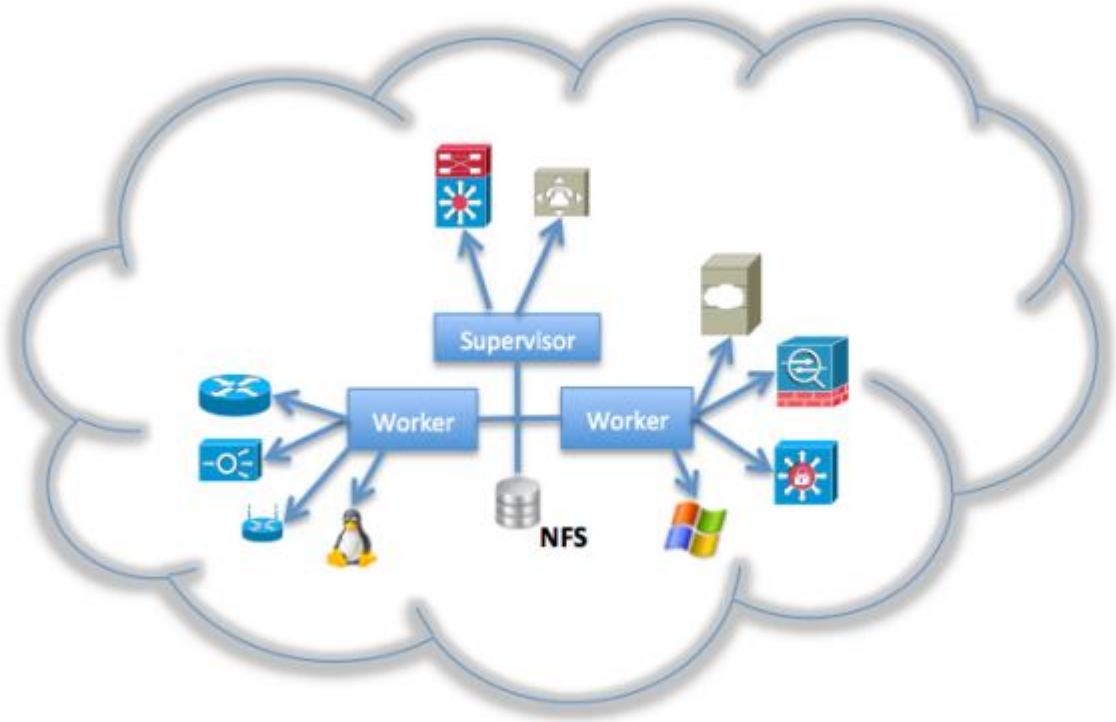


Способы внедрения



- **Внедрение все-в-одном**
  - Весь спектр действий по сбору, анализу, корреляции событий, текущему мониторингу и отслеживанию возникающих инцидентов реализуется одним устройством
  - Наиболее простой способ внедрения
- **Архитектурные элементы**
  - **Супервизор**
  - **Windows Agent(s) and Manager(s)**

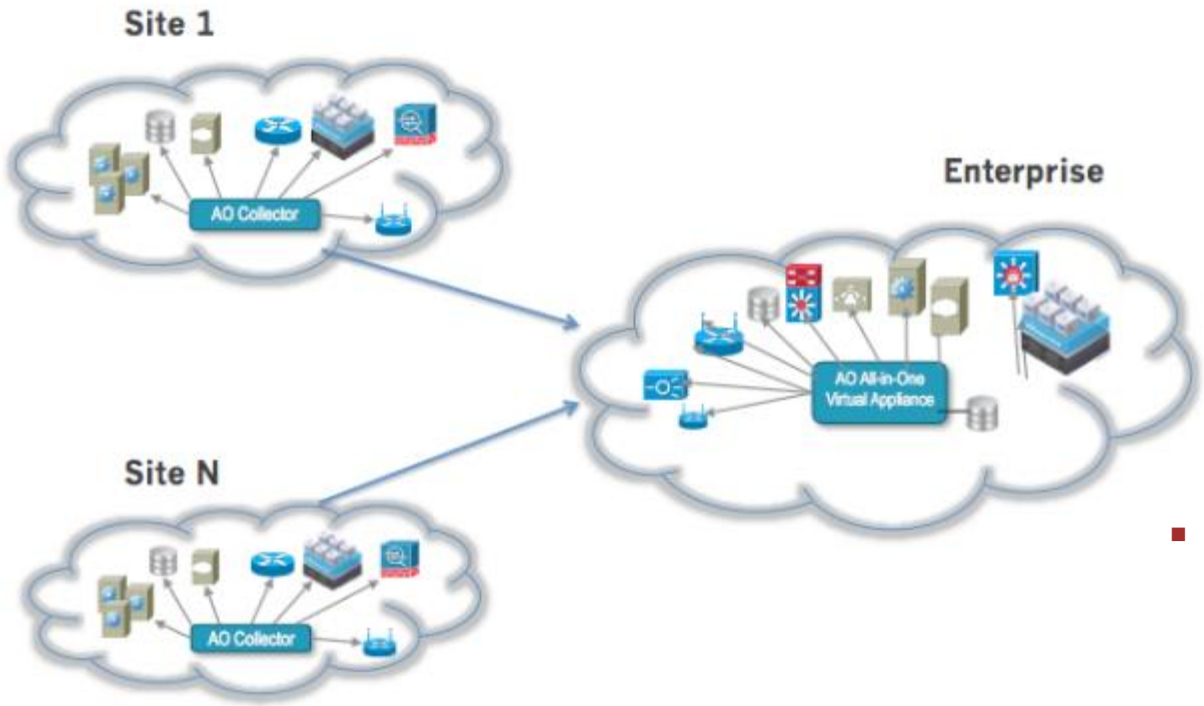
Способы внедрения



- **Частично распределенное внедрение**
  - В составе корпоративной инфраструктуры в дополнение к супервизору разворачивается один или несколько обработчиков
  - Весь спектр действий по сбору, анализу, корреляции событий, текущему мониторингу и отслеживанию возникающих инцидентов распределяется между супервизором и обработчиками
  - Используется общая база данных

- **Архитектурные элементы**
  - **Супервизор**
  - **Обработчики (workers)**
  - **Windows Agent(s) and Manager(s)**

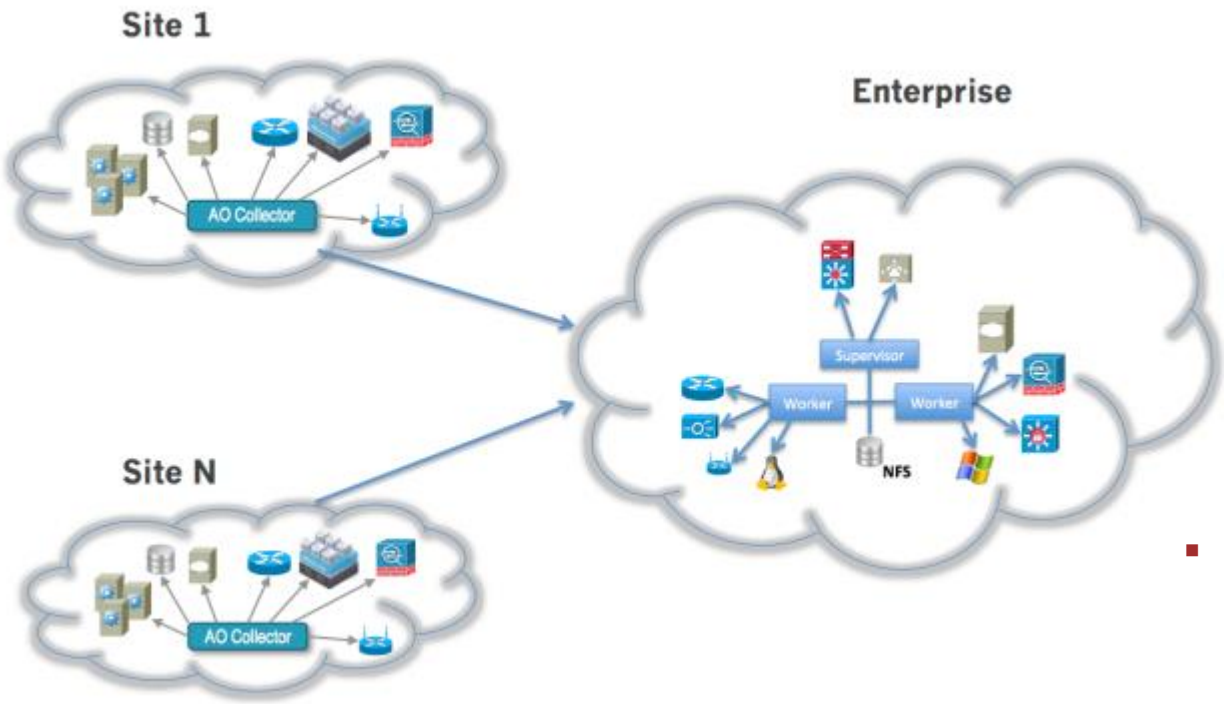
Способы внедрения



- **Распределенное внедрение**
  - » В составе корпоративной инфраструктуры в дополнение к супервизору разворачивается один или несколько коллекторов, размещаемых на удаленных площадках
  - » Весь спектр действий по сбору, анализу, корреляции событий, текущему мониторингу и отслеживанию возникающих инцидентов реализуется супервизором
  - » Коллекторы осуществляют сбор и первичную обработку логов и событий на площадках установки для дальнейшей передачи нормализованного потока событий на супервизор

- **Архитектурные элементы**
  - » **Супервизор**
  - » **Коллекторы**
  - » **Windows Agent(s) and Manager(s)**

Способы внедрения

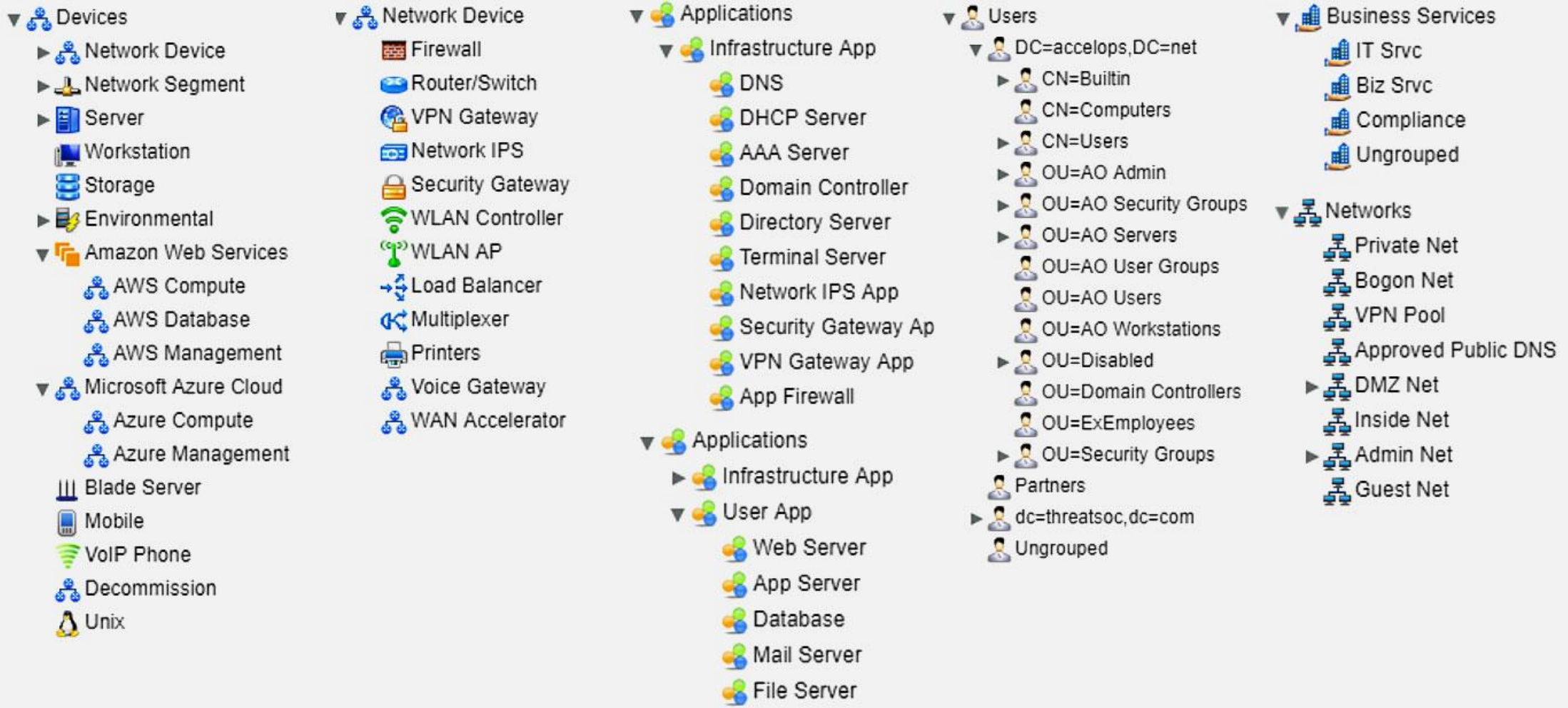


- **Распределенное внедрение с обработчиками**
  - В составе корпоративной инфраструктуры в дополнение к супервизору разворачивается один или несколько обработчиков и один или несколько коллекторов
  - Весь спектр действий по сбору, анализу, корреляции событий, текущему мониторингу и отслеживанию возникающих инцидентов распределяется между супервизором и обработчиками
  - Используется общая база данных
  - Коллекторы осуществляют сбор и первичную обработку логов и событий на площадках установки для дальнейшей передачи нормализованного потока событий на супервизор и обработчики

- **Архитектурные элементы**
  - **Супервизор**
  - **Обработчики (workers)**
  - **Коллекторы**
  - **Windows Agent(s) and Manager(s)**

Функциональность FortiSIEM

CMDB: Устройства, приложения, пользователи, сервисы



Детектирование и исправление

- Аналитика в реальном времени
- Библиотка исправлений (SOC Playbook)
- База данных конфигураций устройств (CMDB)
- Внешние базы угроз
- Динамически добавляемы и настраиваемые парсеры логов

Отчетность о соответствии

- Множество (более 100) различных отчетов о соответствии
  - PCI – HIPAA – FERPA - FISMA
  - SOX, NERC, COBIT, ITIL,
  - ISO, GLBA, GPG13
  - NIST, SANS Critical Controls
- Использовании информации CMDB для:
  - Отслеживания изменений конфигураций устройств
  - Мониторинг пользователей (состава и активности)
  - Контроль целостности файлов

Мониторинг бизнес-сервисов

- Группировка устройств и приложений из базы CMDB в «Бизнес-сервисы»
- Вывод динамических «дашбордов» и виджетов о состоянии заданного «Бизнес-сервиса»
- Оперативное отслеживание подверженных рискам «Бизнес-сервисов» на случай выхода из строя того или иного устройства или приложения
- Мониторинг текущего физического состояния:
  - Устройства: SNMP & APIs
  - Приложения: Synthetic Transactions
- Опци оповещения

Вопросы?


FORTINET