Лучшие практики ИБ от Oberig-IT:

- FUDO PAM
- Fidelis Deception
- предиктивный RBVM Tenable
- классификация данных Titus
- защита от вымогателей Veritas

Максим Прахов
Руководитель развития бизнеса по странам СНГ и Грузии

Oberig it

Oberig IT в Казахстане

- Oberig IT – динамично развивающийся ИТ-дистрибьютор, изначально выстроивший работу в проектном формате и обладающий ресурсами для реализации полного цикла проектов (от тестирования до внедрения)
- 2 офиса в Казахстане, локальная техническая команда с успешным опытом реализации крупных проектов
- Oberig IT занимается развитием проектов передовых ИТ/ИБ решений мирового уровня
- Oberig IT выполняет поставки решений только через реселлер-партнеров

Oberig IT для партнеров в Казахстане это:

- Возможность развития компетенций и новых проектов с высокой маржинальностью
- Гарантия защиты в проектах
- Собственный технический ресурс и полный цикл поддержки развития проекта
- Лидогенерация и продвинутые маркетинговые инструменты (рассылки, вебинары, викторины, CRM)

Oberig it

PAM – мониторинг действий и контроль работы привилегированных пользователей (администраторов важных и критичных ИТ-систем)

Oberig it

FUDO SECURITY

Listed in Gartner's 2018
Magic Quadrant for Privileged
Access Management

Gartner

Почему PAM – это важно?

Если у вас есть права администратора, вы можете делать в ИТ-среде организации все что угодно. Доступ дает пользователю возможность управлять жизненно важными системами фирмы - поэтому мониторинг привилегированного доступа так необходим в практически каждой организации.

Исследования показывают, что PAM становится одной из наиболее важных областей кибербезопасности:

По данным InfoSecurity, практически 100% продвинутых атак, независимо от своего происхождения, связаны с кражей и использованием привилегированных учетных записей.[1]

Gartner определил управление привилегированными учетными записями как проект безопасности № 1 для CISO.[2]

Verizon в своем отчете расследования уязвимости данных за 2018 г. выделяет злоупотребление привилегированным доступом как второй по частоте инцидент.[3]

Вызовы 2020

Выживание бизнеса в условиях изоляции

1. Удаленная работа сотрудников
2. Сокращение затрат

Новые реалии – новые вызовы для эффективности ведения бизнеса

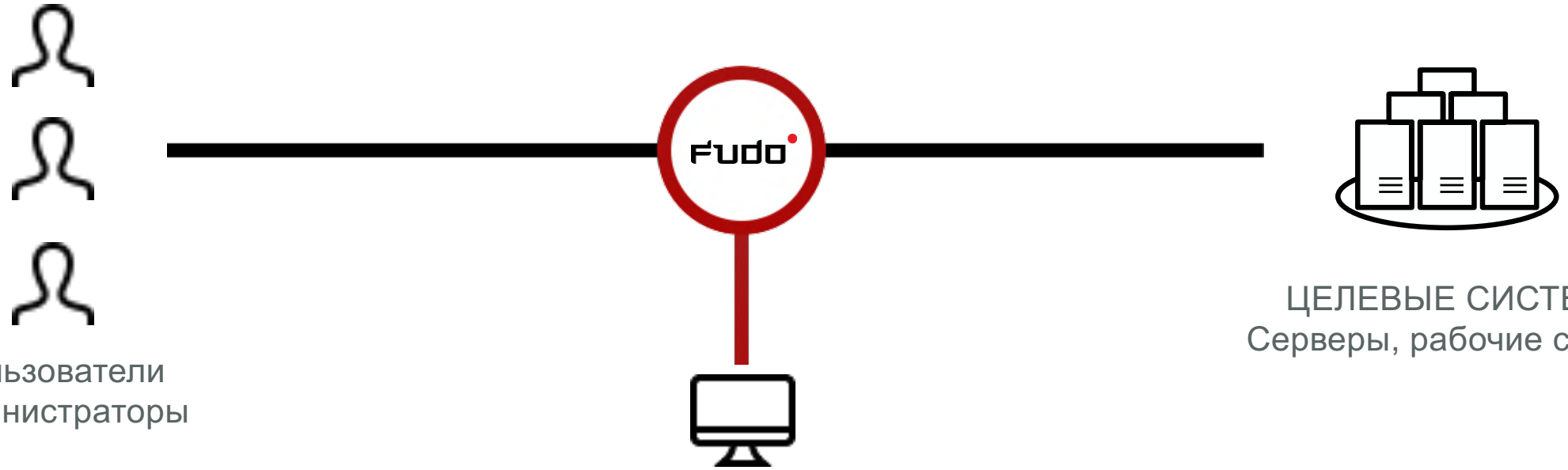
Вызовы 2020

Контроль работы субподрядчиков

- Отсутствие возможности проверить время реально потраченное на оказание услуги
- Дороговизна и не обязательная эффективность оказываемых услуг

Решение – запись всех действий пользователя с возможностью воспроизведения видео и поиска активности/слов (через OCR)
Позволяет проверить активность и реальное время работы

Как работает FUDO PAM



Пользователи
Администраторы

ЦЕЛЕВЫЕ СИСТЕМЫ
Серверы, рабочие станции

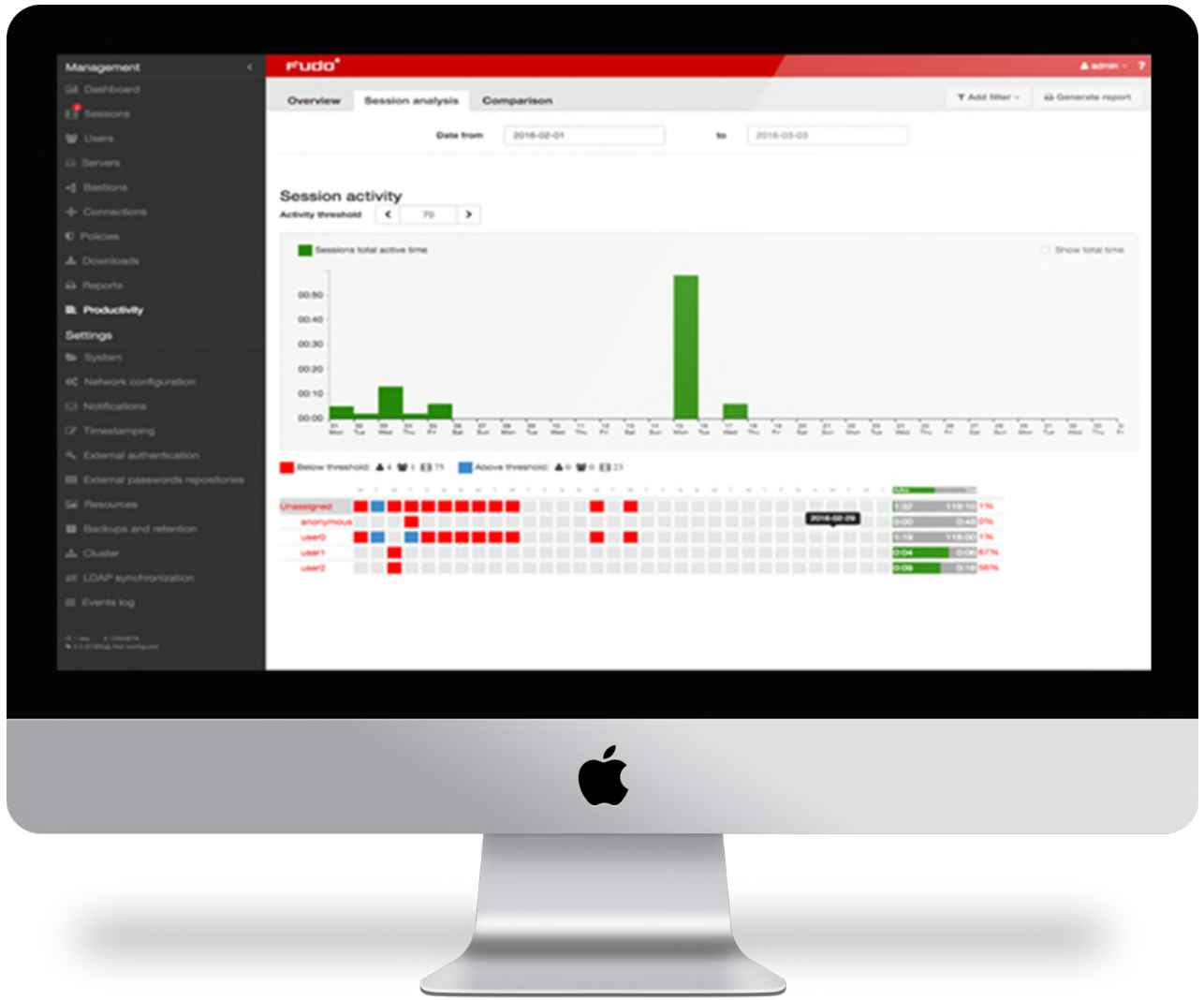
Готовый образ виртуальной машины FUDO

Безагентский контроль по протоколам - управление привилегированным доступом, в том числе пользователями, учетными записями и удаленными сессиями

Oberig it

FUDO SECURITY

FUDO PAM – встроенный анализ продуктивности

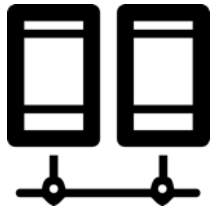


- Видимость активности пользователей
- Видимость активности организации
- Сравнение продуктивности пользователей
- Построение удобных отчетов

Oberig it

FUDO SECURITY

FUDO PAM: особенности и сценарии применения



Простота внедрения, работа с различными целевыми системами по различным протоколам, контроль/предотвращение действий

Уменьшение времени расследования инцидентов

Экономия ресурсов на управлении паролями и использовании политик изменения паролей

Возможность использования для обучения при работе с системами (запись интерактивного видео для новых сотрудников)

Быстрый возврат инвестиций за счет повышения эффективности аутсорсинга и работы ИТ-подразделения

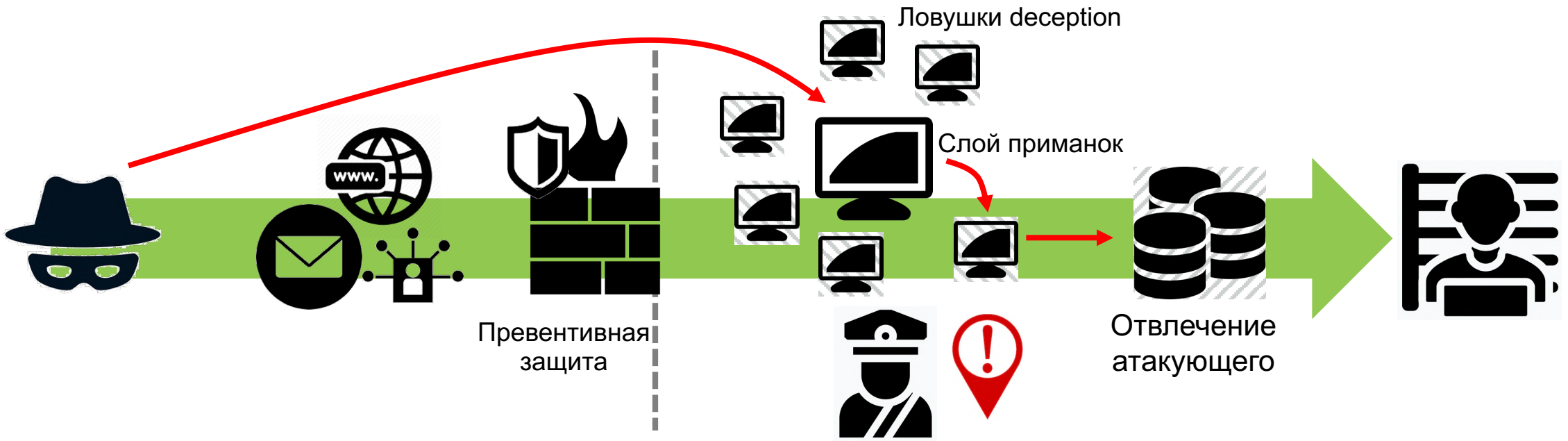
Защита администраторов (доказательства того, что не допускали ошибок при работе)

Oberig it

FUDO SECURITY

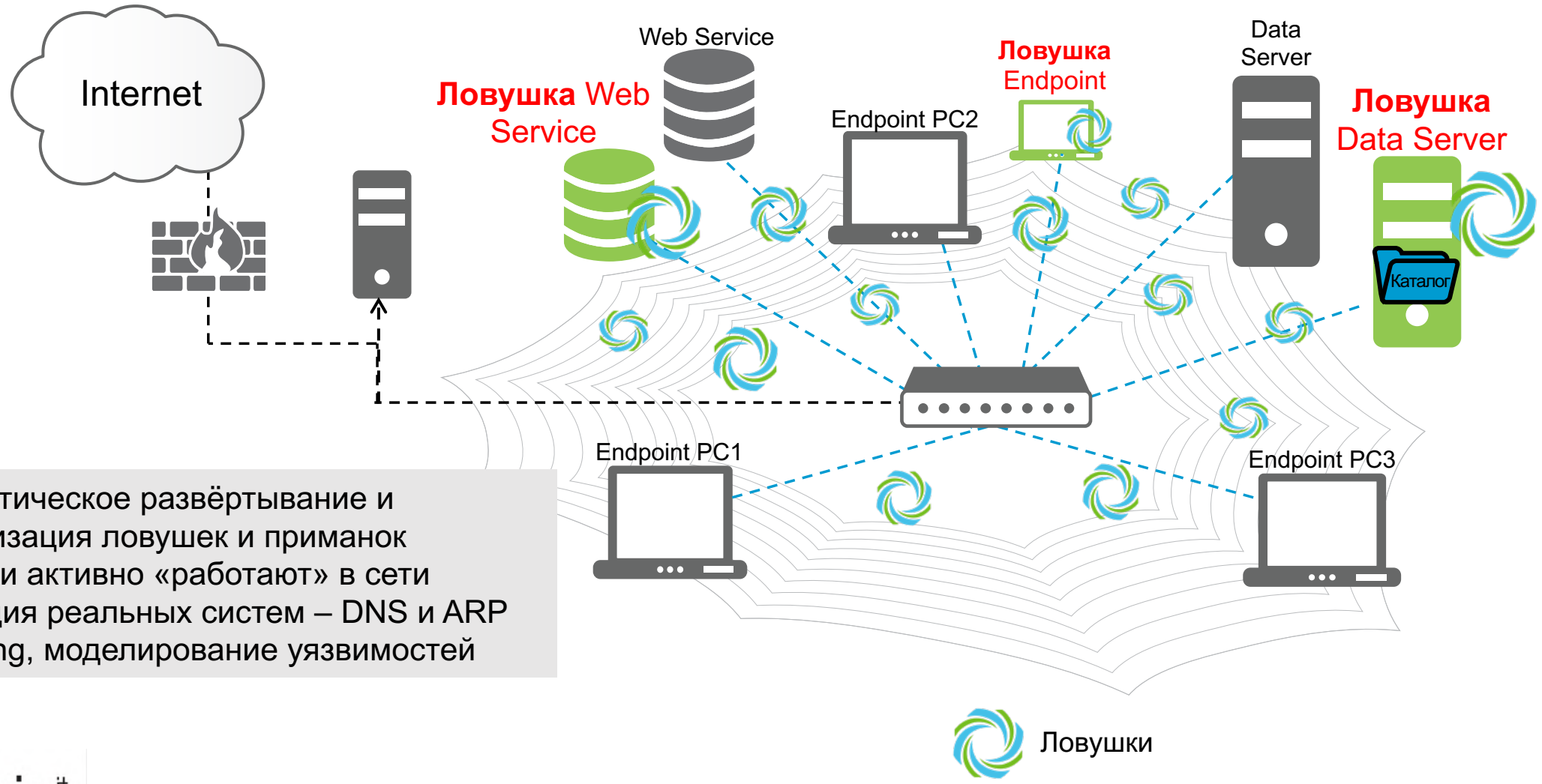
Distributed Deception Platform

Зная, как действуют злоумышленники мы создаем возможности для активной обороны



Oberig it

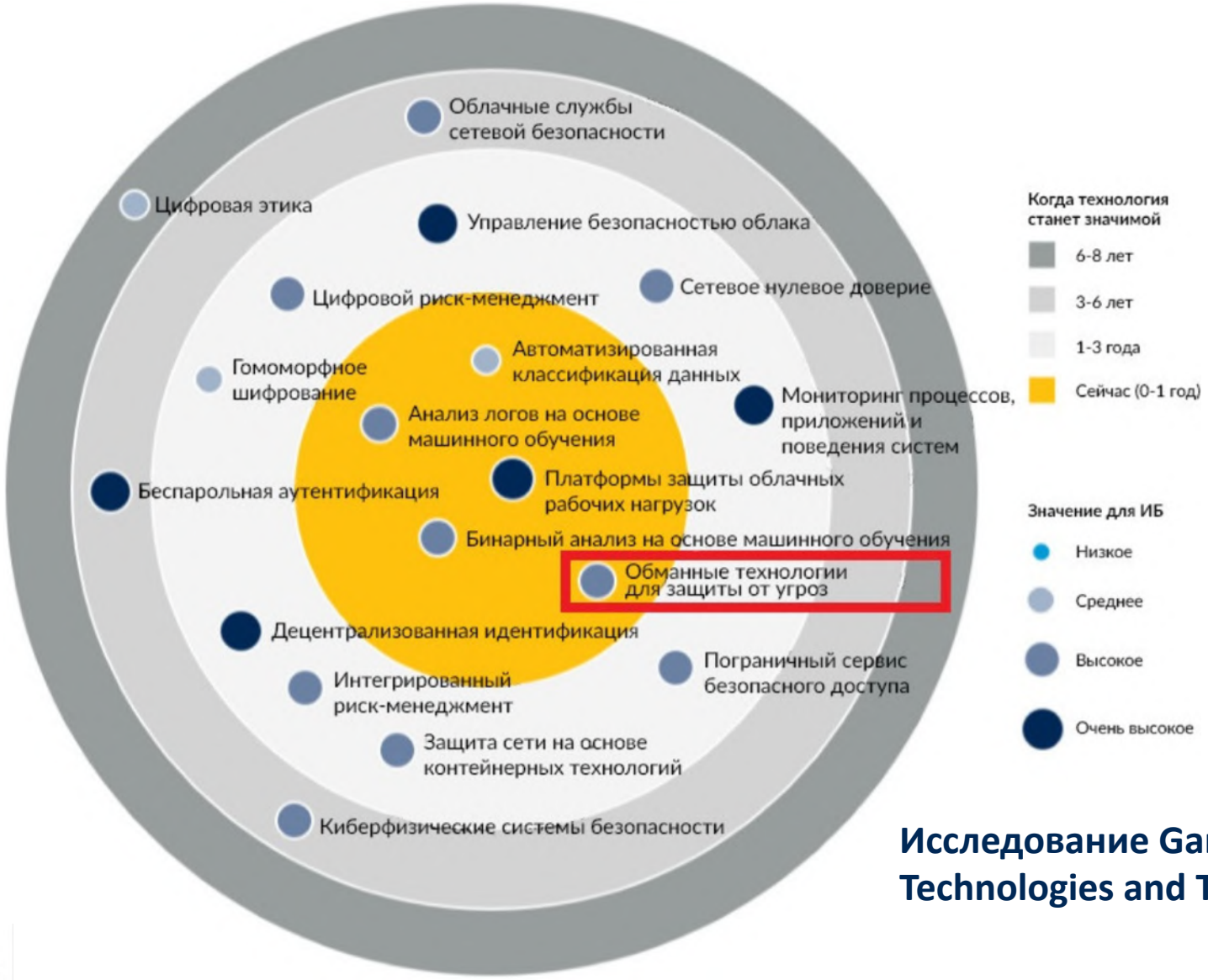
Fidelis Deception – автоматическое создание слоя обманной инфраструктуры



- Автоматическое развёртывание и актуализация ловушек и приманок
- Ловушки активно «работают» в сети
- Имитация реальных систем – DNS и ARP poisoning, моделирование уязвимостей

Oberig it

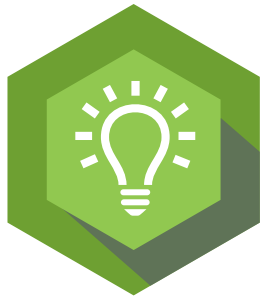
Deception – самый перспективный класс решений ИБ



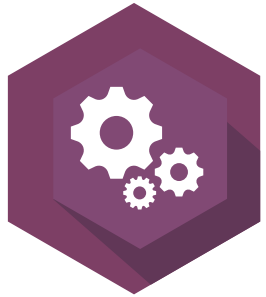
Исследование Gartner 2019 «Emerging Technologies and Trends Impact Radar: Security»

Oberig it

Преимущества технологии Deception

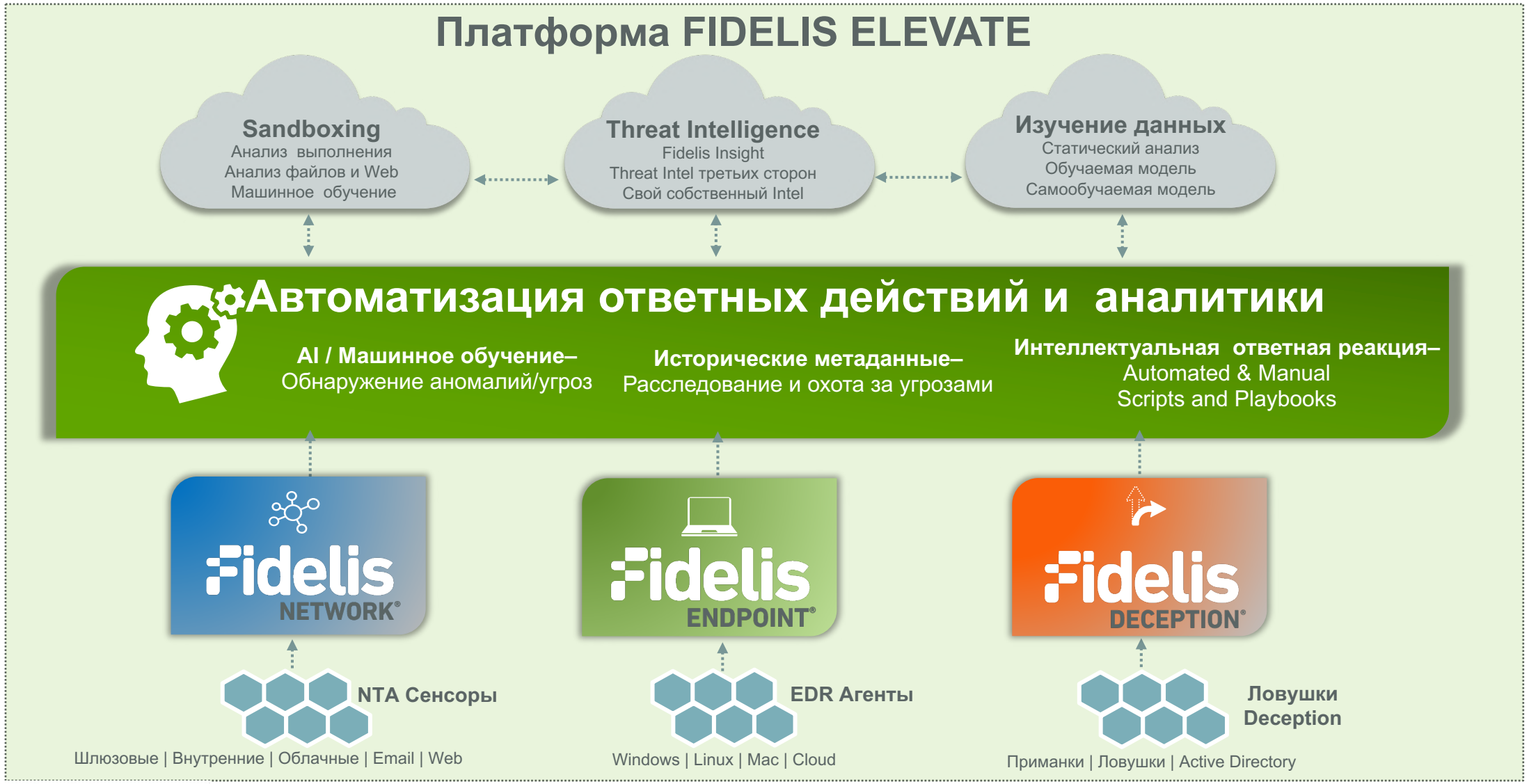


- Инциденты ИБ без ложных срабатываний!
- Защита даже от неизвестных угроз
- Искусство обмана – экспертиза в платформе
- Универсальная защита – от базовых до продвинутых угроз (APT)



- Автоматизация развертывания и адаптация под изменения ИТ
- Простота эксплуатации – несколько часов в неделю
- Без влияния на реальную инфраструктуру
- Эмуляция широкого перечня оборудования и сервисов

Управляемый центр безопасности – Интегрированный, Автоматизированный и Коррелированный



Oberig it

tenable | RESEARCH

30%
Инвестиции в R&D и инновации

139
Уязвимостей нулевого дня в 2019

>54K
Покрытие CVE и 140,000+ плагинов

<24h
Среднее время на выпуск новых плагинов

#1

Доля рынка

ТОЧНОСТЬ и ВЫЯВЛЕНИЕ АТАК НУЛЕВОГО ДНЯ

tenable

Oberig it

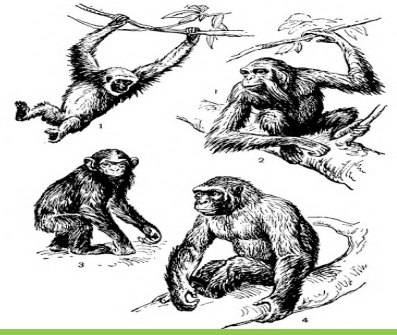
Ежегодный рост выявления новых уязвимостей

- **17313 уязвимостей в 2019**
- **Почти в 3 раза больше новых уязвимостей, в сравнении с предыдущими годами**

tenable®

Oberig it


Ежегодный рост хакерских атак
уязвимостей ВСЕГДА В РАЗЫ БОЛЬШЕ,
чем возможностей их устранения службами ИБ и ИТ
мы НЕ СМОЖЕМ ПОБЕДИТЬ в этой войне
но мы СМОЖЕМ ВЫСТОЯТЬ!
tenable
Oberig it



Эволюция Tenable

Традиционный Vulnerability Management	RISK-BASED Vulnerability Management
Основан на **теоретических** данных	**Практические** данные про уязвимости коррелированные с **хакерской активностью и критичностью** актива
Фокус только на **IT**	**IT + Apps, Cloud, Agents, OT & Containers**
Статическое значение CVSS	**Динамический** рейтинг, ежедневное обновление
Реактивное реагирование	**Проактивное** реагирование
Политики и поддержка аудита	**Приоритизация и поддержка стратегических решений**, политики, поддержка аудита

tenable®

Oberig it

Решения Titus для защиты корпоративных данных

ВОСТАНОВЛЕНИЕ И КОНТРОЛЬ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ

Titus Classification Suite

Добавьте необходимый контекст к локальным и облачным данным с помощью ведущего решения для классификации данных.

ИДЕНТИФИКАЦИЯ ЧУВСТВИТЕЛЬНЫЕ ДАННЫХ

Titus Illuminate

Сканируйте и анализируйте неструктурированные данные в «состоянии покоя" и применяйте соответствующие метрики.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Titus Accelerator For Privacy

Обнаружение личной информацию (PII) при создании почтового сообщения или файла. На основе машинного обучения.

ОПРЕДЕЛЕНИЕ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ В ЭЛЕКТРОННОЙ ПОЧТЕ

Titus Data Identification

Облачное решение для защиты данных электронной почты с предварительно настроенными библиотеками для легкого развертывания.

ШИФРОВАНЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Titus Encryption
Powered by Virtru

Контролируйте доступ к своим ценным данным с помощью гибкого интегрированного решения для шифрования.

TITUS A HelpSystems Company

Oberig it

Titus – автоматизация и упрощение защиты данных

ИДЕНТИФИКАЦИЯ

Интеллектуальное машинное обучение
обнаружение конфиденциальных данных

КЛАССИФИКАЦИЯ

Гибкие политики, мощный движок
для классификации ваших данных

TITUS POLICY
ENGINE
METADATA
APIS

ЗАЩИТА

Защитите данные при создании,
в состоянии покоя и в процессе

- Безопасный обмен
- Утечка данных
- Интеллектуальная блокировка
- Повышенная безопасность
- Автоматическая категоризация
- Соответствие нормативным требованиям

TITUS
A HelpSystems Company

Oberig it

VERITAS устойчивость к вирусам-шифровальщикам

Реалии 2020: защита бэкапов – последний рубеж обороны!

Специализированный вебинар 3.12

https://www.veritas.com/en/uk/form/webinar/ransomware-resilience-in-a-multicloud-era

Ransomware attacks are a growing threat, with 42% of companies reporting that they've faced at least one attack. On average, companies have 4.5 attacks.

Oberig it

VERITAS

Устойчивость к вирусам-шифровальщикам

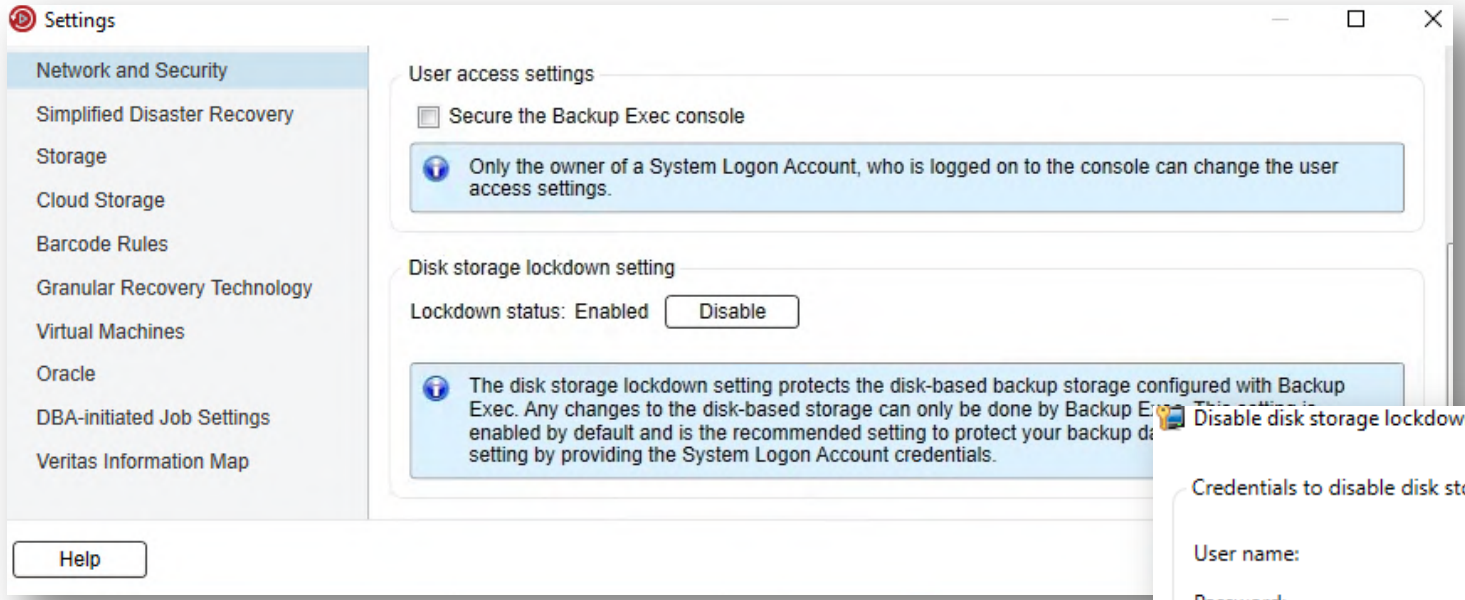
Два механизма защиты дисковых систем хранения данных от атак вирусов-шифровальщиков:

- Только доверенные процессы Backup Exec могут записывать данные в дисковое хранилище (добавлено в Backup Exec 20.4)
- Внешнему коду запрещено выполнять процессы Backup Exec (ограничение добавлено в Backup Exec 21)

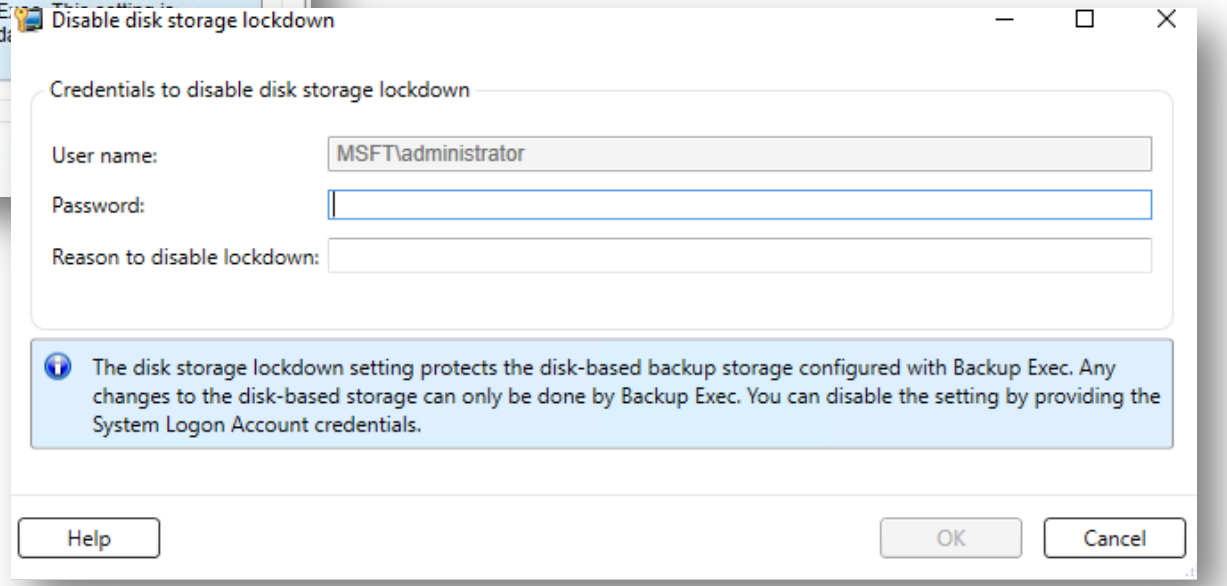
Платить или не платить вымогателям ?!

Oberig it VERITAS

Блокировка хранилища включена по-умолчанию



Нажатия кнопки Включить/Отключить регистрируются в журнале аудита и журнале событий

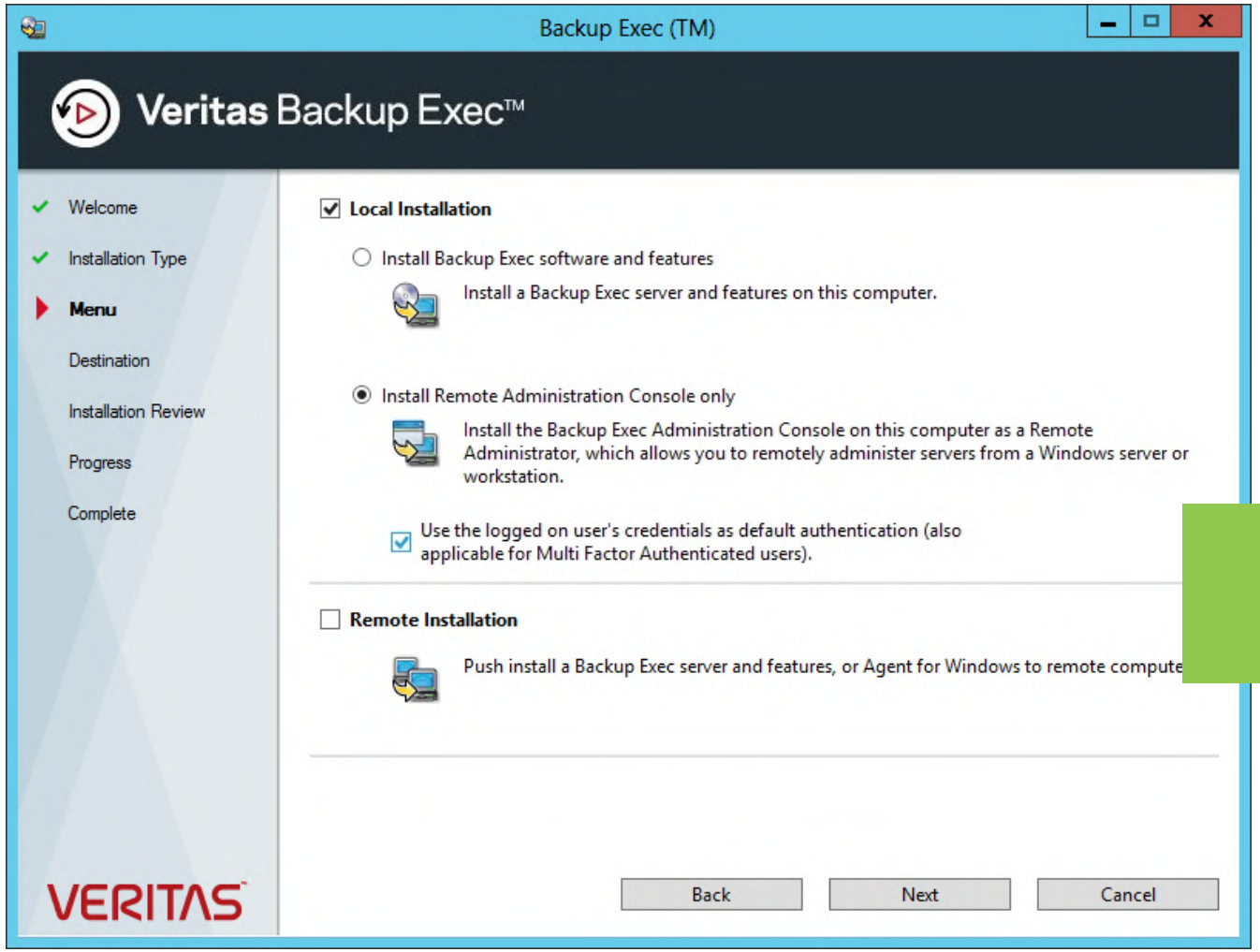


Требуется ввод данных системной учетной записи

Oberig it

VERITAS

Двухфакторная аутентификация – удаленное администрирование



Если флажок установлен, то по умолчанию SSO включен в окне подключения

Fidelis Cybersecurity

Как найти злоумышленников в Вашей ИТ-инфраструктуре?

ОБМАНУТЬ. ОБНАРУЖИТЬ. УДЕРЖАТЬ. ОТРАЗИТЬ.

Платформа Fidelis Elevate - автоматическое обнаружение целенаправленных атак и действий инсайдеров без ложных срабатываний: на конечных точках, сетевом оборудовании, устройствах IoT и в облачных средах!

FIDELISSECURITY.COM

Oberig it

Компания Oberig IT
официальный дистрибьютор решений Fidelis
на территории Украины, Грузии и стран СНГ
oberig-it.com

Максим Прахов
Руководитель развития бизнеса в странах СНГ
m.prakhov@oberig-it.com
+7 (917) 570-87-38