Безопасность должна быть удобной:
Как с помощью PAM системы реализовать концепцию Zero Trust и при этом не вызвать негодование сотрудников.

Илья Горюнов ig@afi-d.ru

13.10.2021

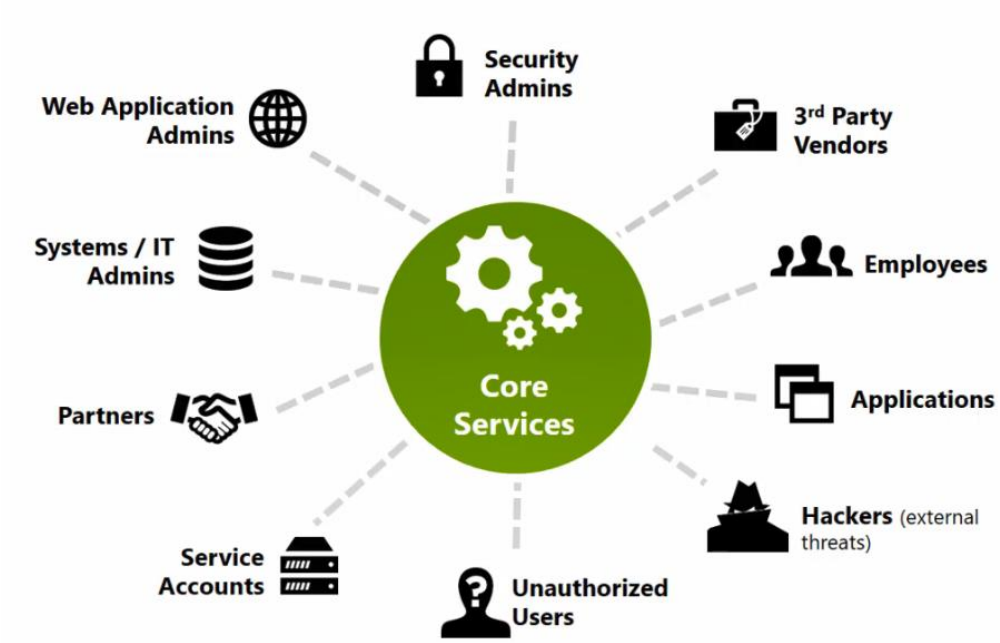
thycotic

Привилегированные учетные записи: что это такое?

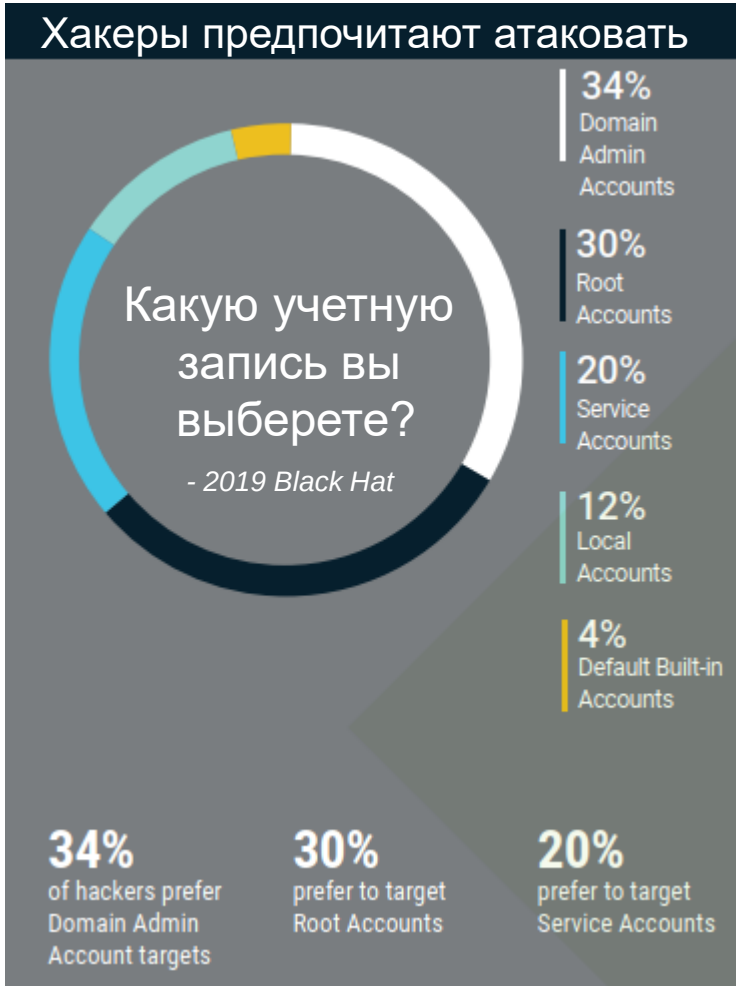
- **Учетные записи с высоким или даже неограниченным доступом** к критичным данным и системам, используемые ИТ персоналом или ИТ системами.
- **Существуют повсюду -** на каждом устройстве, сервере, базе данных, приложении.
- Представляют одну из **наиболее критичных уязвимостей** в ИТ инфраструктуре организации.

Используя привилегированную учетную запись можно:

- Украсть или уничтожить информацию
- Остановить технологические или бизнес-процессы
- Повредить оборудование
- Совершить мошеннические действия с финансами

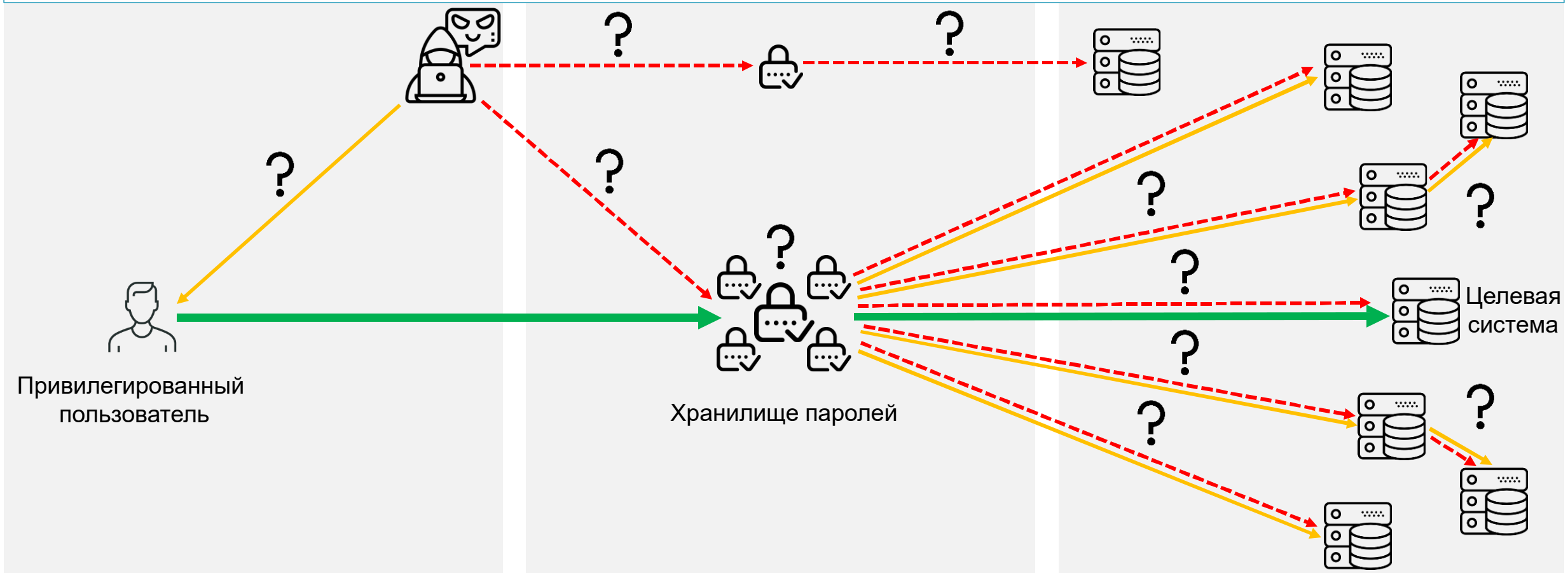


Защита привилегированных учетных записей оказывает наибольшее влияние на информационную безопасность



thycotic

Без **контроля** учетных записей вы не знаете кто ими пользуется



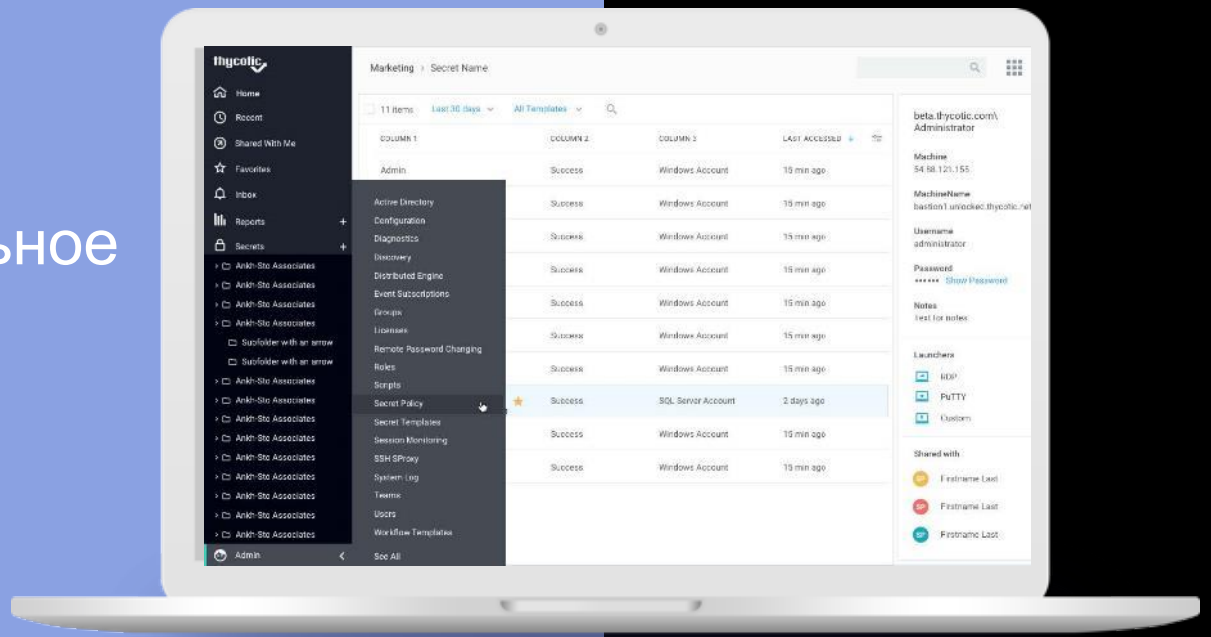
01 ИДЕНТИФИКАЦИЯ | **02 ХРАНЕНИЕ** | **03 ДОСТУП**

Обеспечение принципа **Zero Trust** для всех пользователей

Внедрение принципа **минимальных привилегий** для любого типа доступа

Secret Server

Полнофункциональное PAM решение, доступное как локально так и в облаке



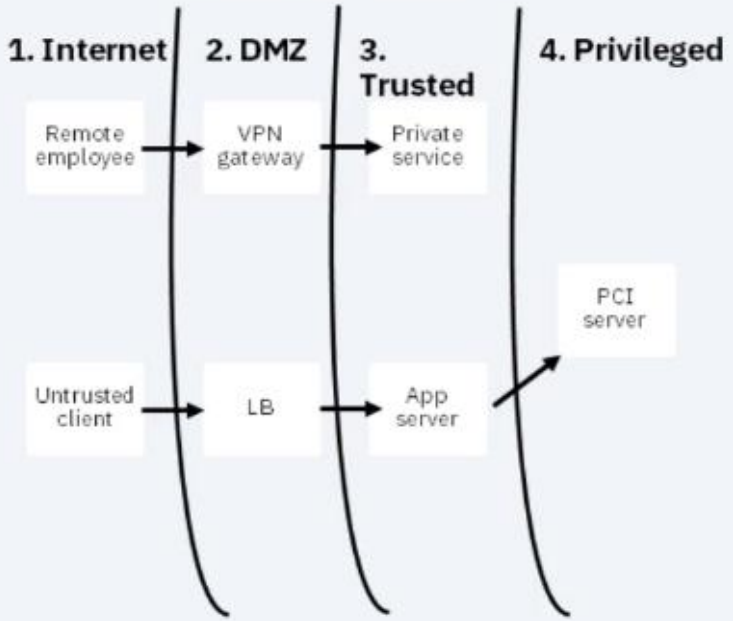
- Установка хранилища
- Обнаружение учетных записей
- Предоставление доступа для внутреннего и внешнего персонала
- Смена паролей
- Обеспечение соблюдения аутентификации Zero-Trust
- Полный контроль и аудит

thycotic

Традиционный подход vs. Zero Trust

Traditional Security Architecture

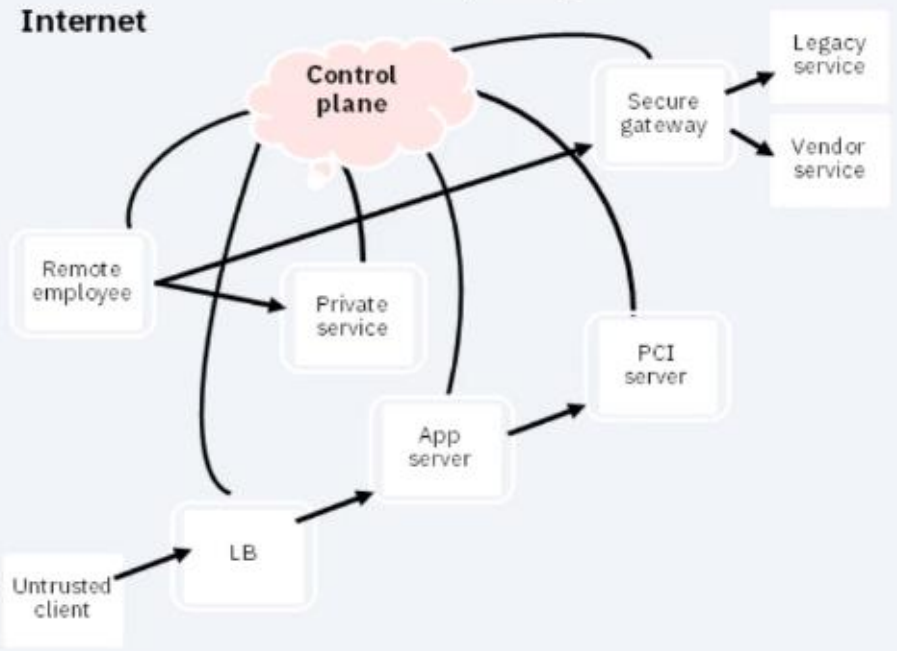
There are 4 zones in a traditional network security architecture:



Vs.

Zero Trust Architecture

The **control plane** in a zero trust architecture allows you to remove those zones, and ultimately enforce least privilege:



thycotic

Как выглядит отсутствие Zero Trust

Характеристика	Состояние
Учетные данные	Для привилегированного доступа используются общие учетки
Парольная политика	Общие статичные пароли, хранятся в экселе или текстовых документах
МФА	Отсутствует
Безопасное окружение	Отсутствует. Доступ к серверам разрешен напрямую с рабочих станций
Мониторинг и аудит	Отсутствует
Процесс согласования доступа	Отсутствует
Принцип минимальных привилегий	Привилегии бинарны, ты либо пользователь либо рут
Принцип минимального доступа	Под одним админом можно получить доступ к любому серверу
Отчетность	Только встроенный аудит
Настройка политик безопасности	Локальные политики безопасности

Три столпа Zero Trust

Всегда проверяйте

Персонализируйте доступ
Без разрастания учетных записей

Подтверждайте права доступа
На вход (МФА) и действия (согласование).

Скрывайте пароли
Сессии можно запускать и не зная их

Меняйте пароли
Как регулярно так и по событию.

Никогда не доверяйте

Минимальные привилегии

Микросегментация
С ролевой моделью доступа

Удалите лишние права.
В домене и на устройствах.

Доверяйте приложениям.
А не пользователям.

И чтобы сотрудникам было удобно

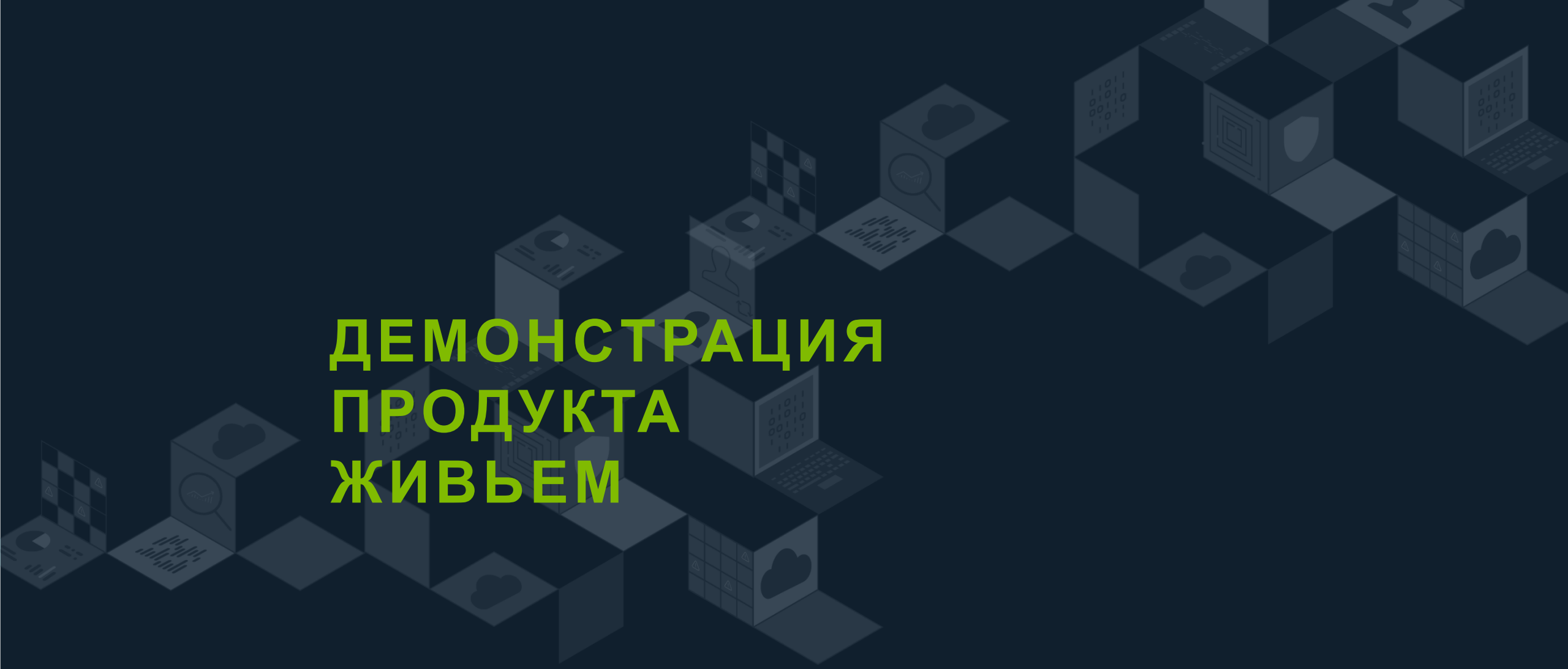
Тотальный контроль

Любая активность записывается.
Как внутри PAM так и внутри сессии

Отслеживайте изменения.
Это потенциальные инциденты.

Реагируйте проактивно.
Даже когда вы спите.

На случай, если все плохо



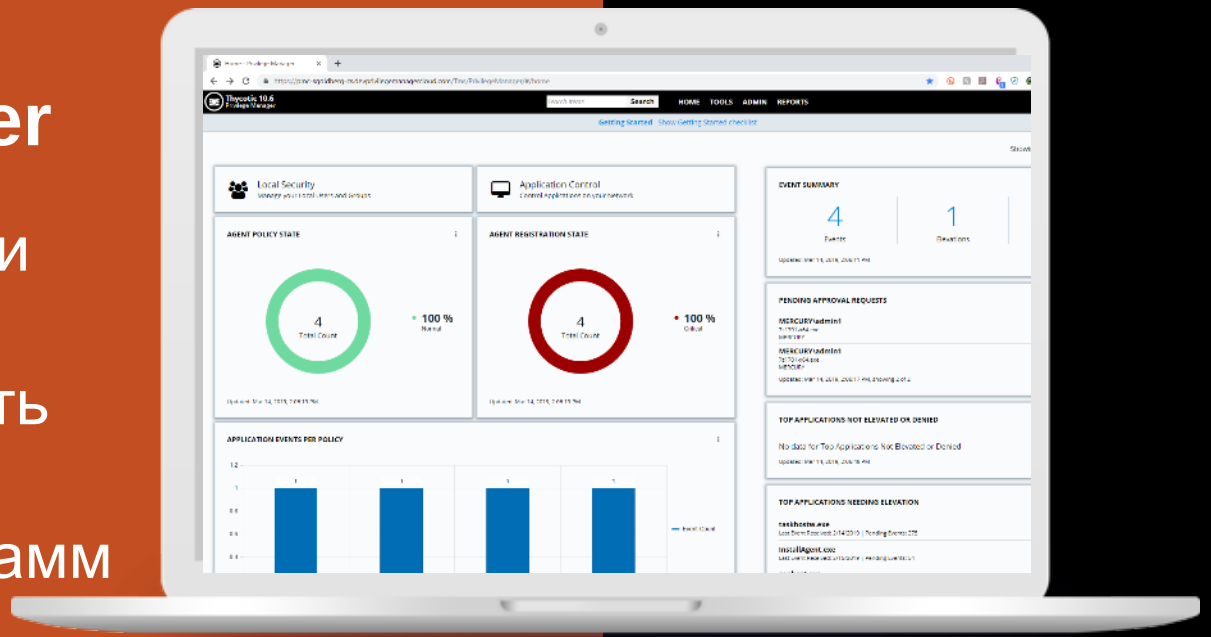
ДЕМОНСТРАЦИЯ ПРОДУКТА ЖИВЬЕМ

Вебинар 23.09.2020

thycotic

Privilege Manager

Защитите серверы и рабочие станции, чтобы предотвратить распространение вредоносных программ



- Управление учетными записями
- Развертывание агентов
- Контроль приложений
- Повышение прав приложений
- Улучшение продуктивности

thycotic

Privilege Manager: от какой угрозы защищает

Учетные записи локальных администраторов на конечных устройствах могут быть использованы для получения доступа к другим компьютерам, доменным ресурсам и критичным службам, если не применяется модель наименьших привилегий

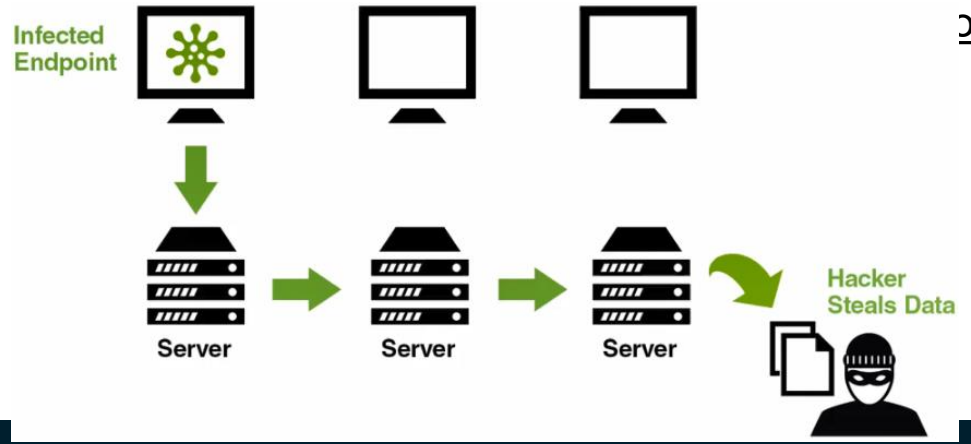
Такие учетные записи есть на каждом устройстве, потому что дать больше прав чем нужно – это гораздо проще, чем гранулировано их настраивать. В результате получаются пользователи с привилегированным доступом

Проблема избыточных привилегий на рабочих станциях сотрудников очень часто выпадает из области внимания ИБ, что делает компанию уязвимой к атакам связанным с повышением прав, такими как pass-the-hash.

Согласно Microsoft

96% критических уязвимостей Windows могут быть устранены удалением административных привилегий

60% всех уязвимостей Microsoft могут быть устранены удалением административных привилегий



Privilege Manager: примеры использования

1. Можно сделать корпоративную общую папку, наполнить ее доверенные приложения и Privilege Manager разрешит обычным пользователям запускать их из этой папки сразу с повышенными правами.

2. Если нужного приложения нет в этой папке, можно создать другую, куда пользователь может скачать приложение из инета, а при попытке запустить Privilege Manager отправит его на virustotal и после прохождения проверки отправит запрос администратору на подтверждение установки.

3. Все остальные приложения, в т.ч. неавторизованные скрипты в почте полностью блокируются, т.е. даже не запускаются

4. Пользователь с административной ролью и ограниченными правами (например подрядчик, поддержка, программист 1С или DBA) при заходе на сервер сможет запустить только ту систему, доступ к которой ему разрешен. Например, WSUS, сервер 1С, сервер БД. Все остальное ему будет недоступно, несмотря на то, что он администратор. Возможно грануляция прав вплоть до, например, типа оснастки в mmc консоли – можно разрешить просмотр сертификатов и запретить просмотр устройств.

5. На удаленных системах с ограниченным сетевым доступом Privilege Manager может осуществлять смену паролей во-первых исходящими подключениями, а во-вторых не только по расписанию но и по событию, например, при логине. Подобный сценарий например был реализован на банкоматах в одном из банков.

Как выглядит наличие Zero Trust

Характеристика	Состояние
Учетные данные	Ведется персонализация и учет использования аккаунтов
Парольная политика	Пароли и SSH ключи ротируются и централизовано хранятся
МФА	Включена для доступа ко всем критичным системам
Безопасное окружение	Доступ к серверам осуществляется через промежуточный прокси либо джамп-хост
Мониторинг и аудит	Сессия записывается, логируется, аудит отправляется в SIEM
Процесс согласования доступа	Внутри PAM либо с помощью внешних ITSM или IGA
Принцип минимальных привилегий	Роли тщательно сконфигурированы
Принцип минимального доступа	Доступ предоставляется на основании согласования
Отчетность	Отслеживается активность с детализацией по пользователю и хосту
Настройка политик безопасности	Централизованное управление политиками на системах

Почему нужно использовать Thycotic?

Все будет по полочкам

Управление учетными записями – это одна из тех задач, с которой нельзя справиться без автоматизации и не сойти с ума.

Лучше всего справляться не «костылями», а инструментом, который был создан именно для этой задачи.

Thycotic существует 15 лет и включен в лидеры «квадранта Гартнера» - его разработчики точно знают, что нужно вашей сети:

- Автоматизация
- Надежность
- Отчетность
- Управляемость

Доступнее и удобнее

Можно установить и настроить за 1 день, самостоятельно без обучения,
а не месяц и за деньги с интегратором, как у конкурента

Для старта требуется всего 1 сервер,
а не 4, как у конкурента.

Все базовые функции работают сразу, без необходимости настройки остальных систем вашей сети,
а не как… ну, вы поняли :)

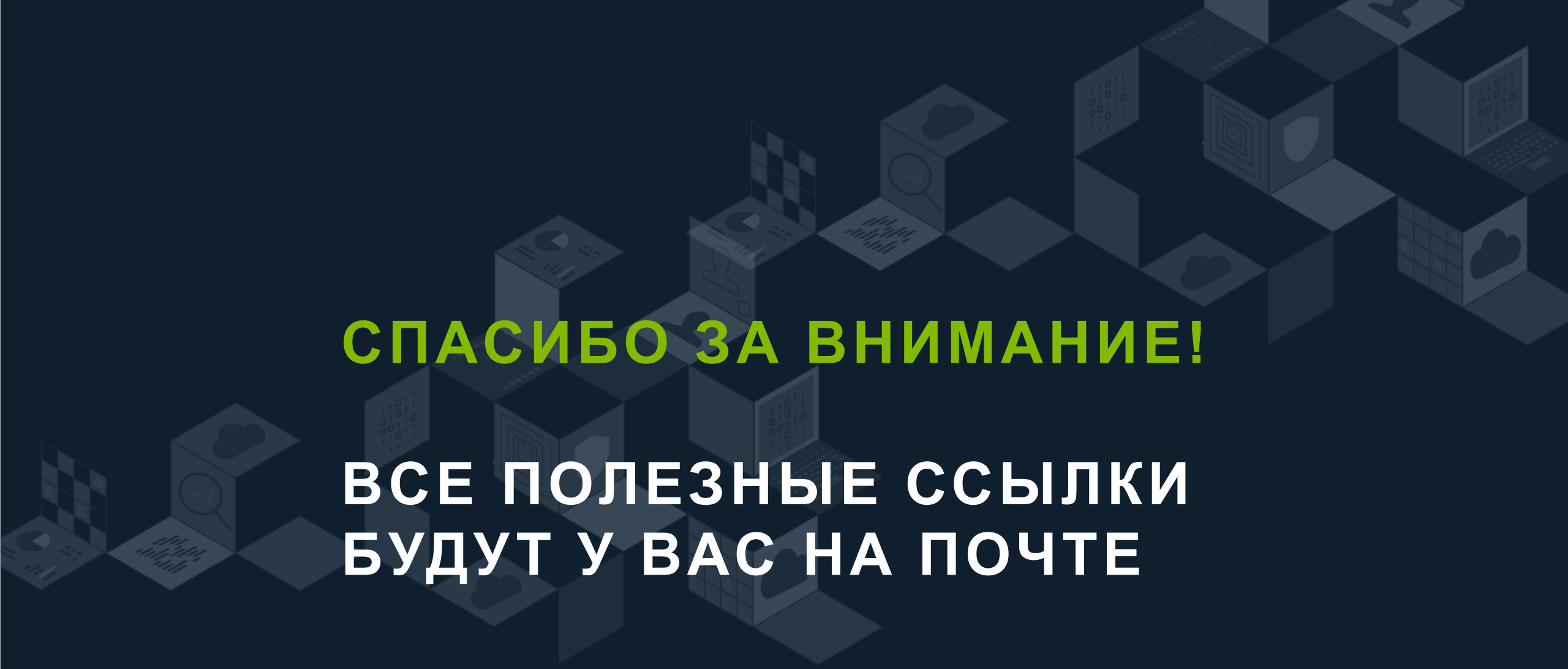
Подойдет для вашей сети

Интегрируется с десятками популярных систем, включая сканеры безопасности, HSM, поставщиков двухфакторной аутентификации

Требует обычного Windows-сервера с IIS и любую версию MS SQL Server, включая бесплатную.

Будет расти вместе с вами: масштабирование для надежности и распределения нагрузки можно настраивать «на ходу», по мере того, как вы приводите вашу сеть в порядок.

Загрузить по ссылке: www.Thycotic.com



СПАСИБО ЗА ВНИМАНИЕ!

ВСЕ ПОЛЕЗНЫЕ ССЫЛКИ БУДУТ У ВАС НА ПОЧТЕ

Илья Горюнов ig@afi-d.ru

13.10.2021

thycotic