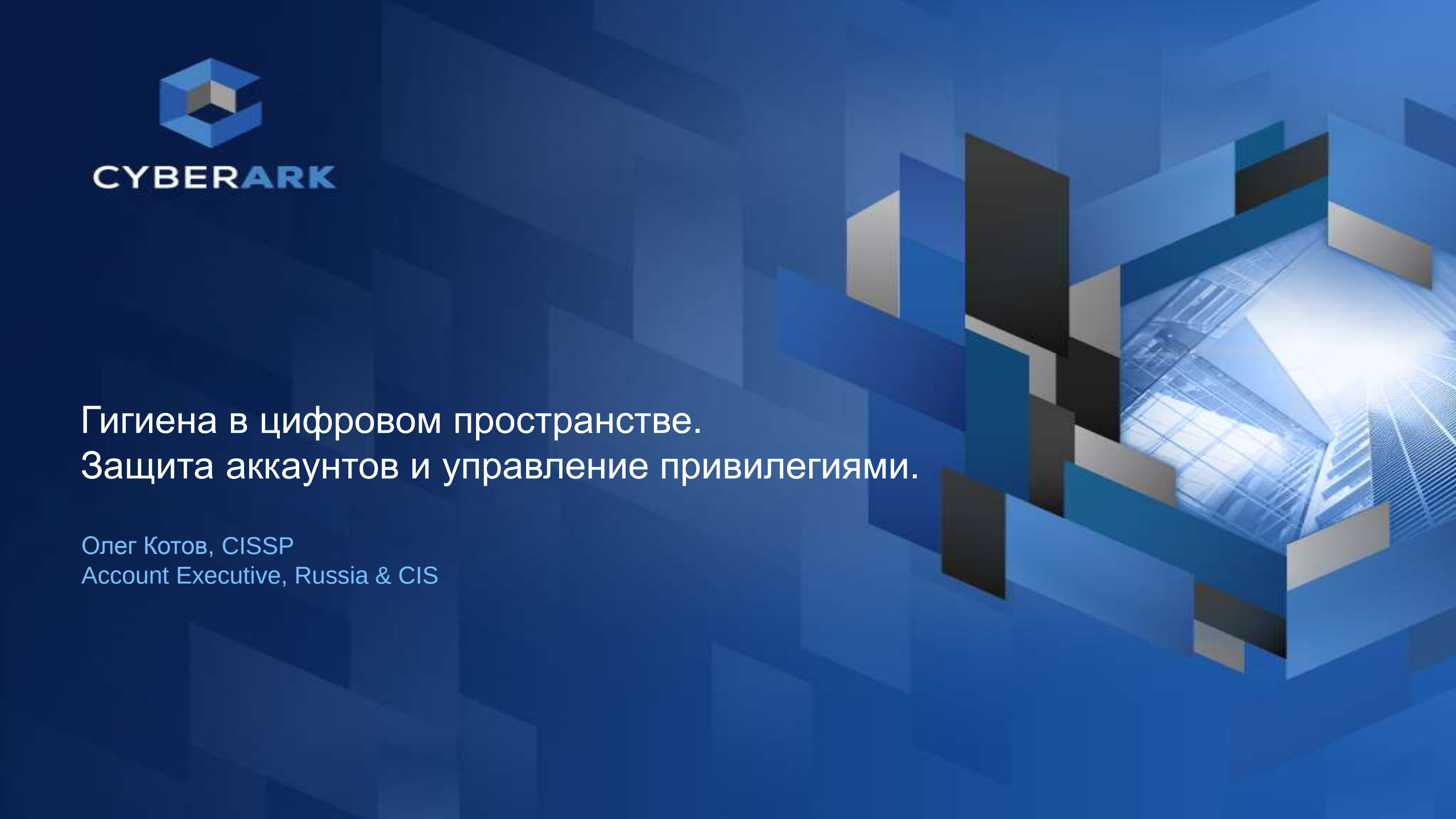


Гигиена в цифровом пространстве.
Защита аккаунтов и управление привилегиями.

Олег Котов, CISSP
Account Executive, Russia & CIS

Как страшно жить …

Манипуляции с учётными данными – неотъемлемая часть атаки

“…100% of breaches involved stolen credentials.”

“APT intruders…prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts.”

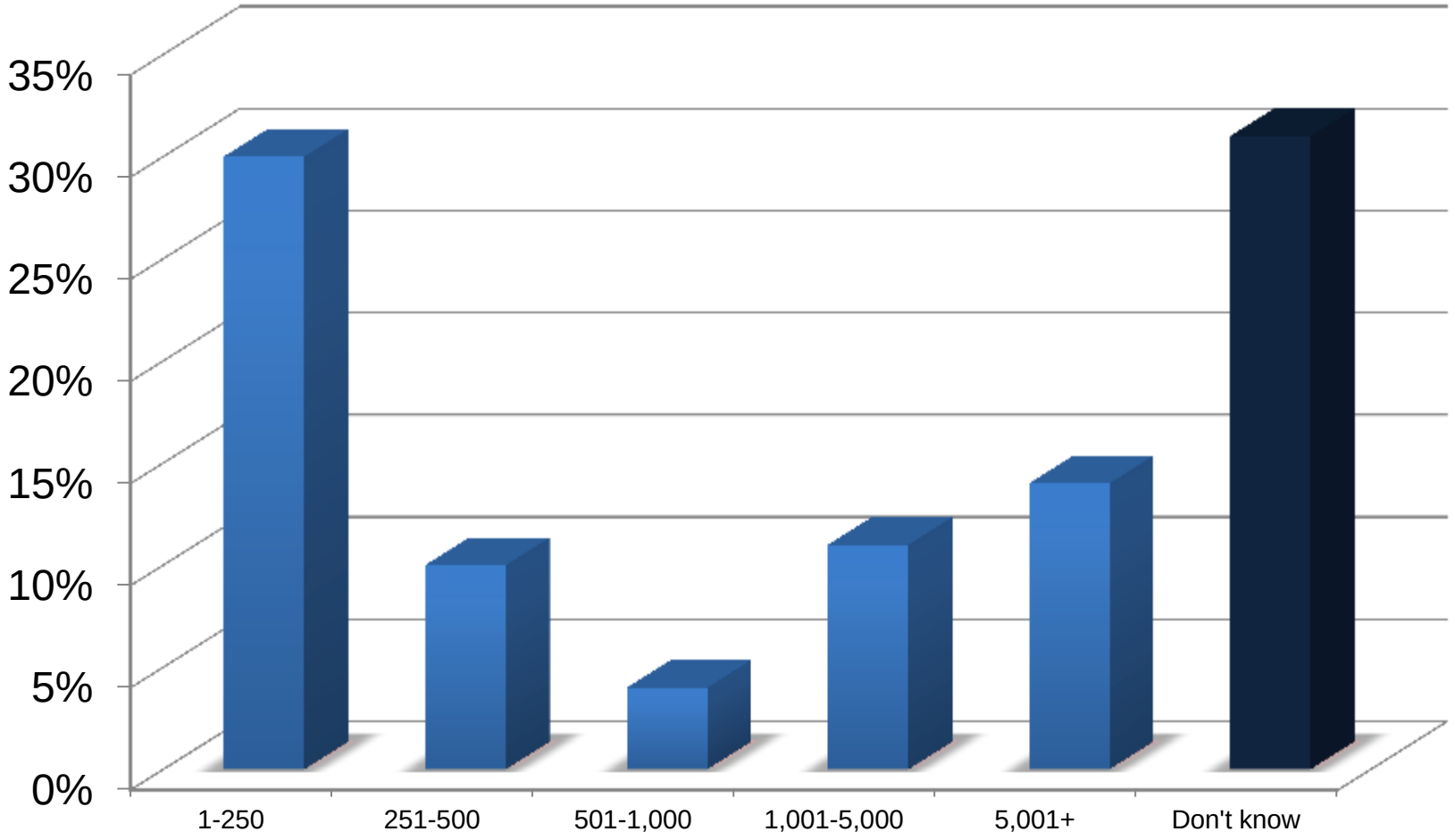
Mandiant, M-Trends and APT1 Report

CYBERARK

Потеря контроля над собственными активами

CYBERARK

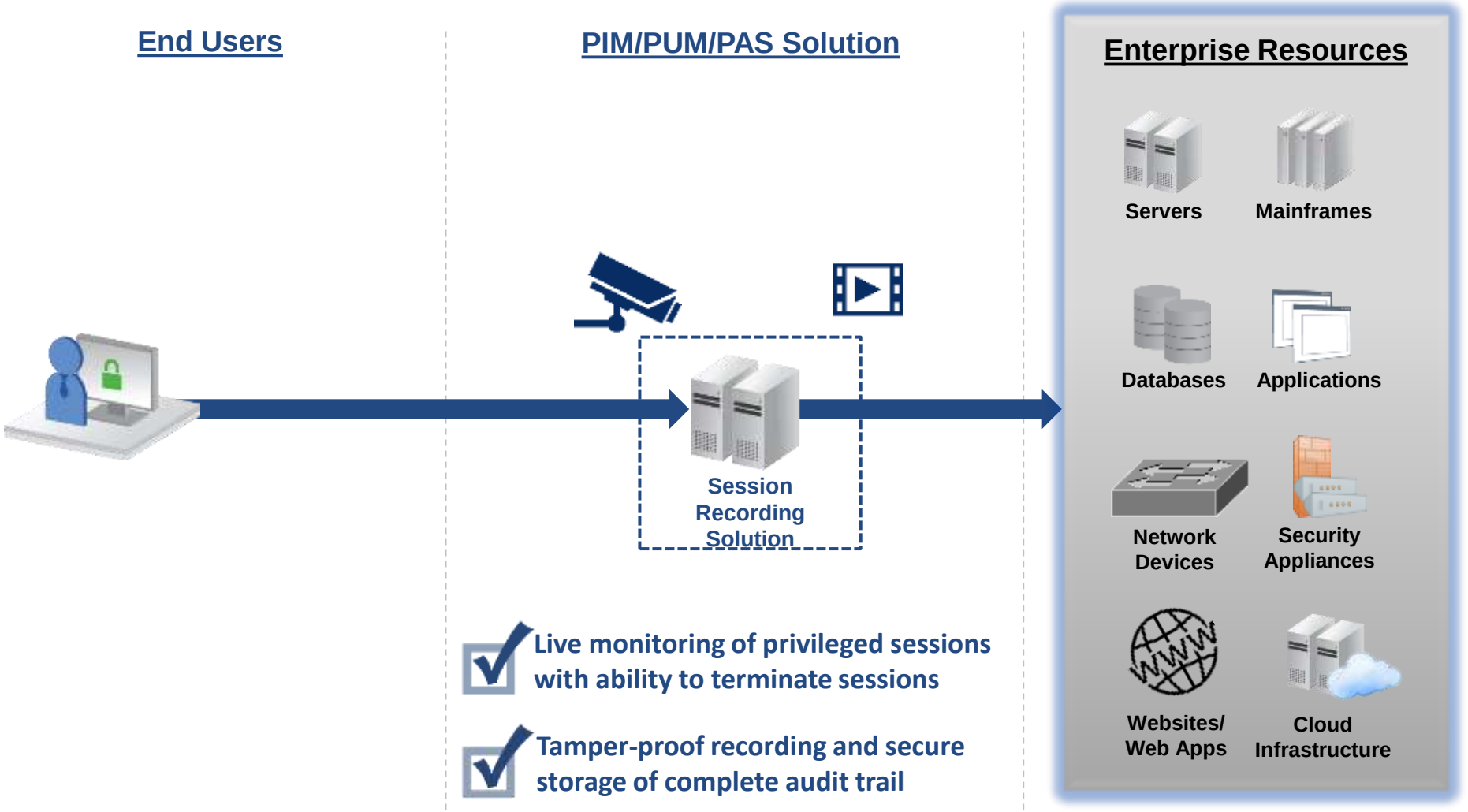
Сколько привилегированных аккаунтов у вас?



Cyber-Privileged Account Security & Compliance Survey, May 2015 (Enterprise > 5000 Employees)

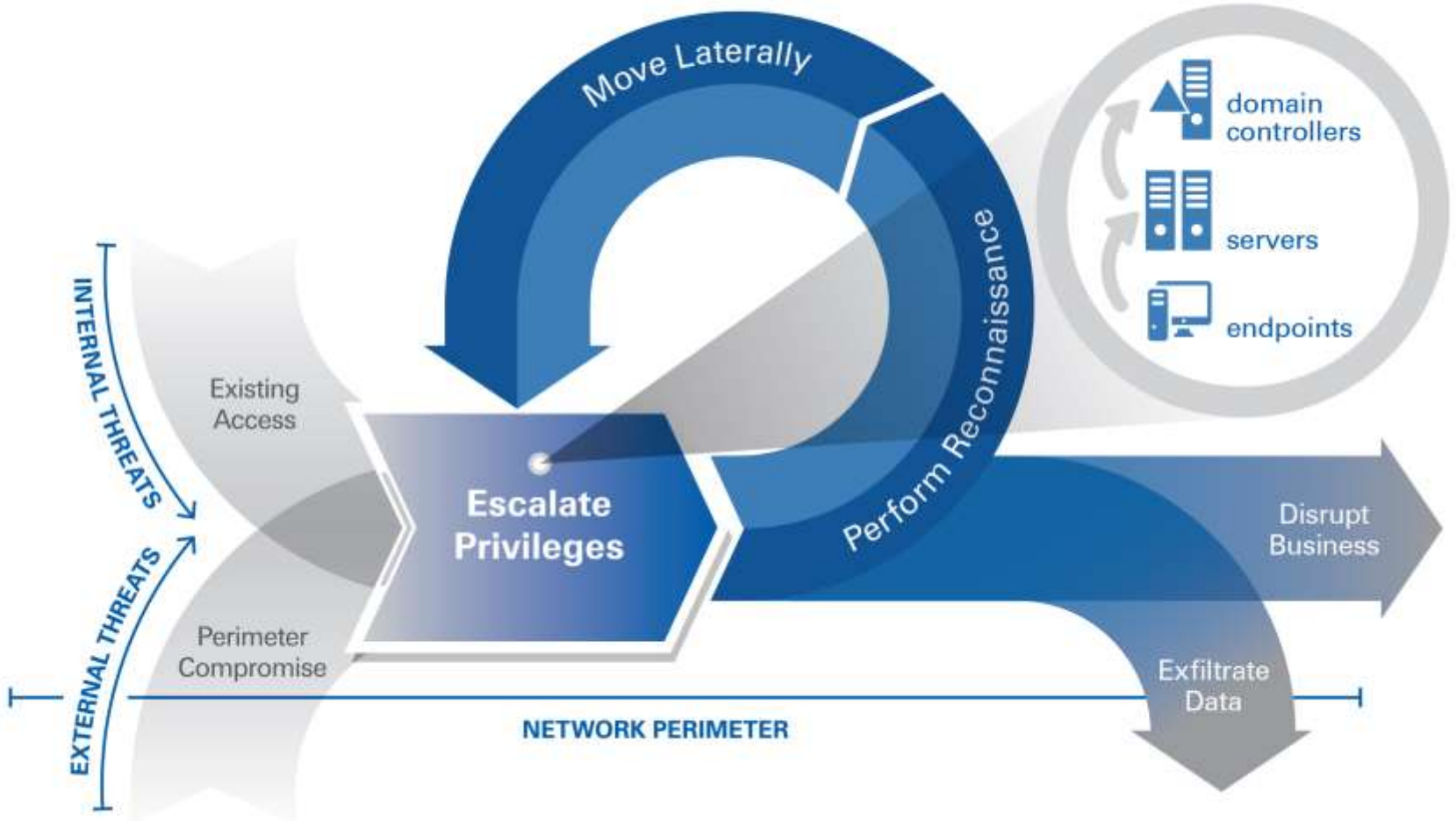
CYBERARK

Классический подход защиты привилегированного доступа



CYBERARK

Полная картина



CYBERARK

Функциональные домены PAS решения

CREDENTIAL PROTECTION & MANAGEMENT

SESSION ISOLATION, MONITORING & RECORDING

THREAT DETECTION & ANALYTICS

***NIX SERVER PROTECTION**

WINDOWS SERVER PROTECTION

DOMAIN CONTROLLER PROTECTION

CYBERARK®

Точка отсчёта

Assess the Required Controls with the Mind-set that the attacker is already on the inside… this is especially true when the threat comes from 3rd Parties or Malicious Insiders

> Because many existing implementations of Active Directory Domain Services have been operating for years at risk of credential theft, organizations **should assume breach** and consider the very real possibility that they may have an undetected compromise of domain or enterprise administrator credentials
>
> **—MICROSOFT,**
> "MITIGATING PASS-THE-HASH AND OTHER CREDENTIAL THEFT, VERSION 2," 2014

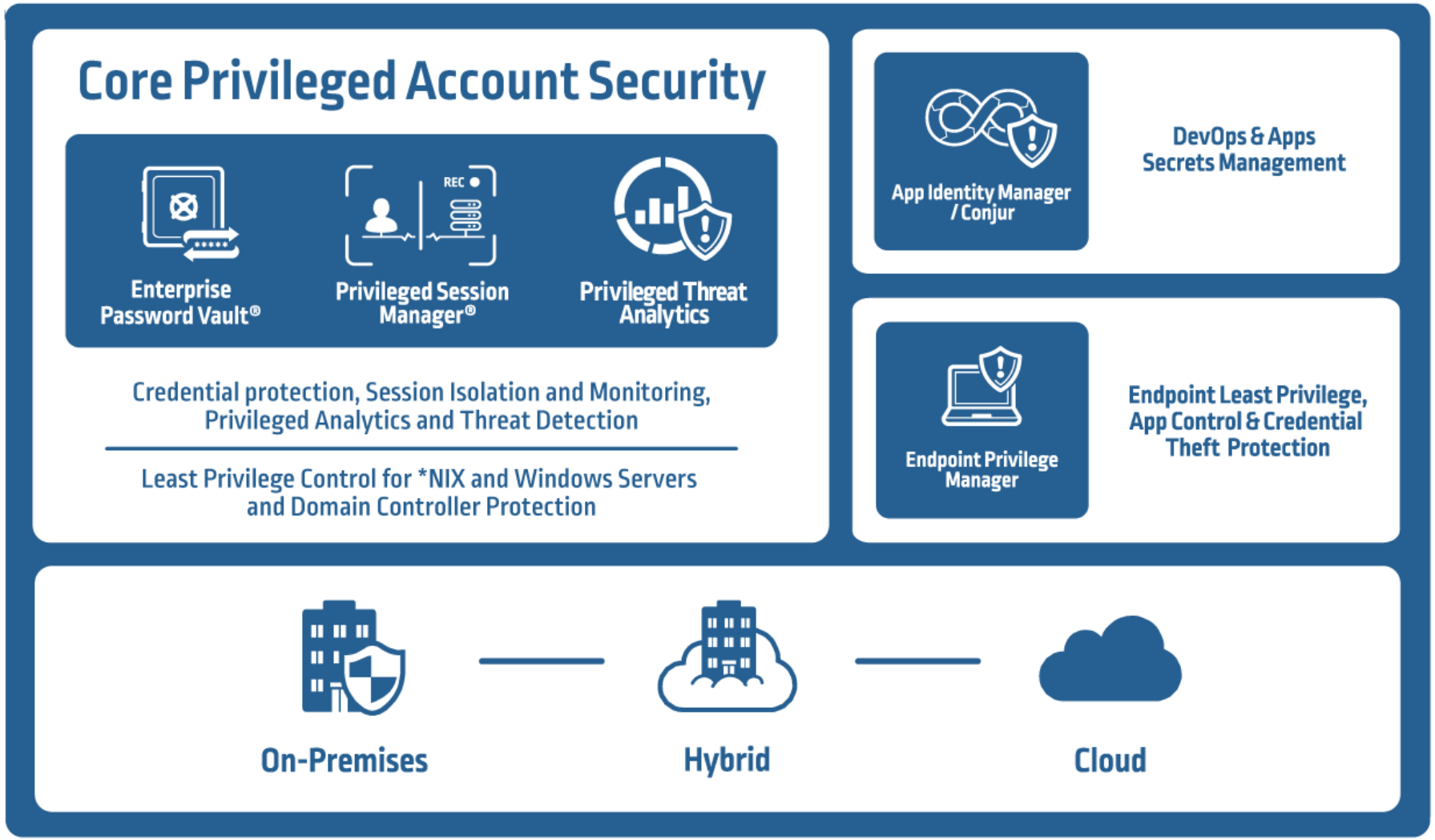
CYBERARK

Программа гигиены работы с привилегиями

Step 1	Сфокусироваться на атаках, позволяющих получить полный контроль над инфраструктурой (например, Kerberos Golden Ticket).
Step 2	Контролировать и обезопасить инфраструктурные аккаунты.
Step 3	Минимизировать возможности скрытого перемещения злоумышленника по инфраструктуре.
Step 4	Защитить аккаунты от сторонних платформ.
Step 5	Управлять SSH ключами доступа к критичным Unix серверам.
Step 6	Защита в облаках и DevOps.
Step 7	Защита аккаунтов критичных для бизнеса.

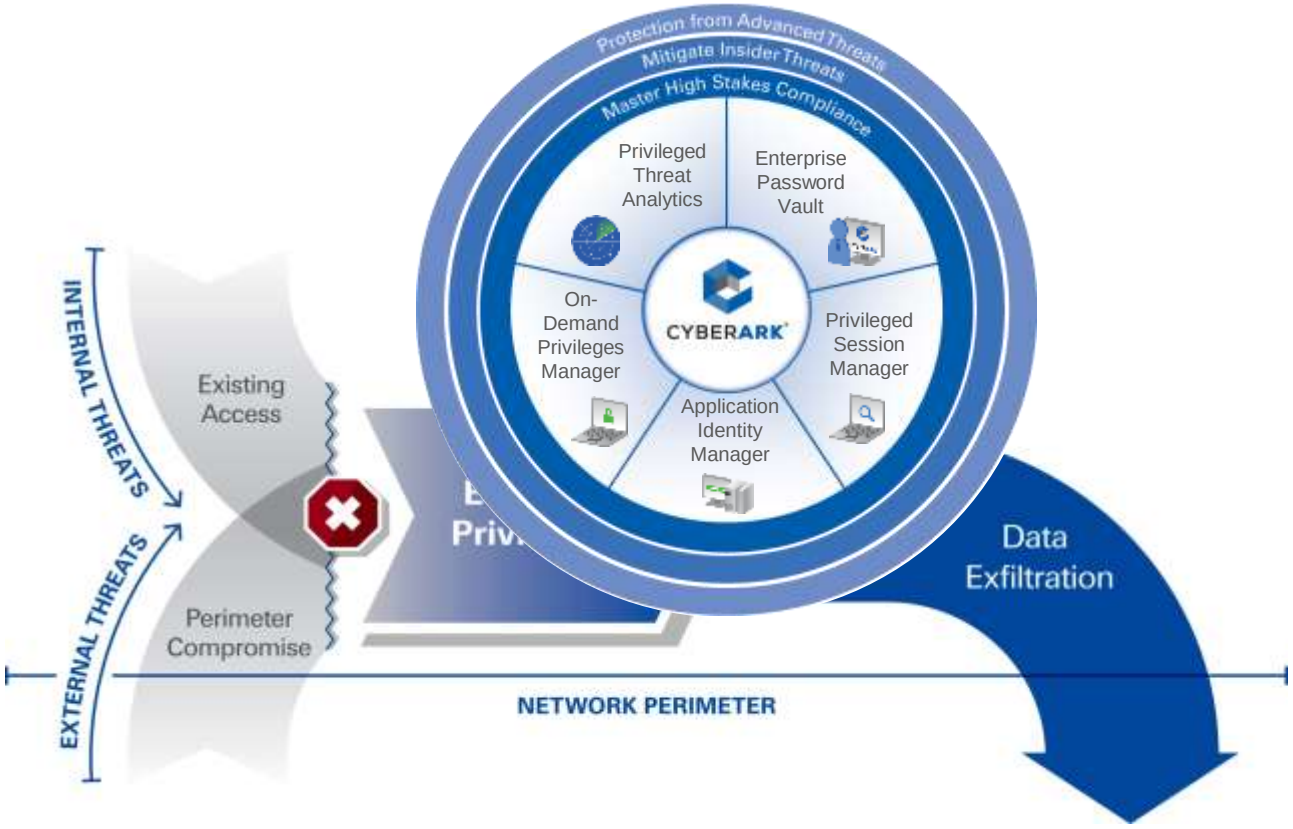
CYBERARK

CyberArk Privileged Account Security



CYBERARK®

Комплексный подход

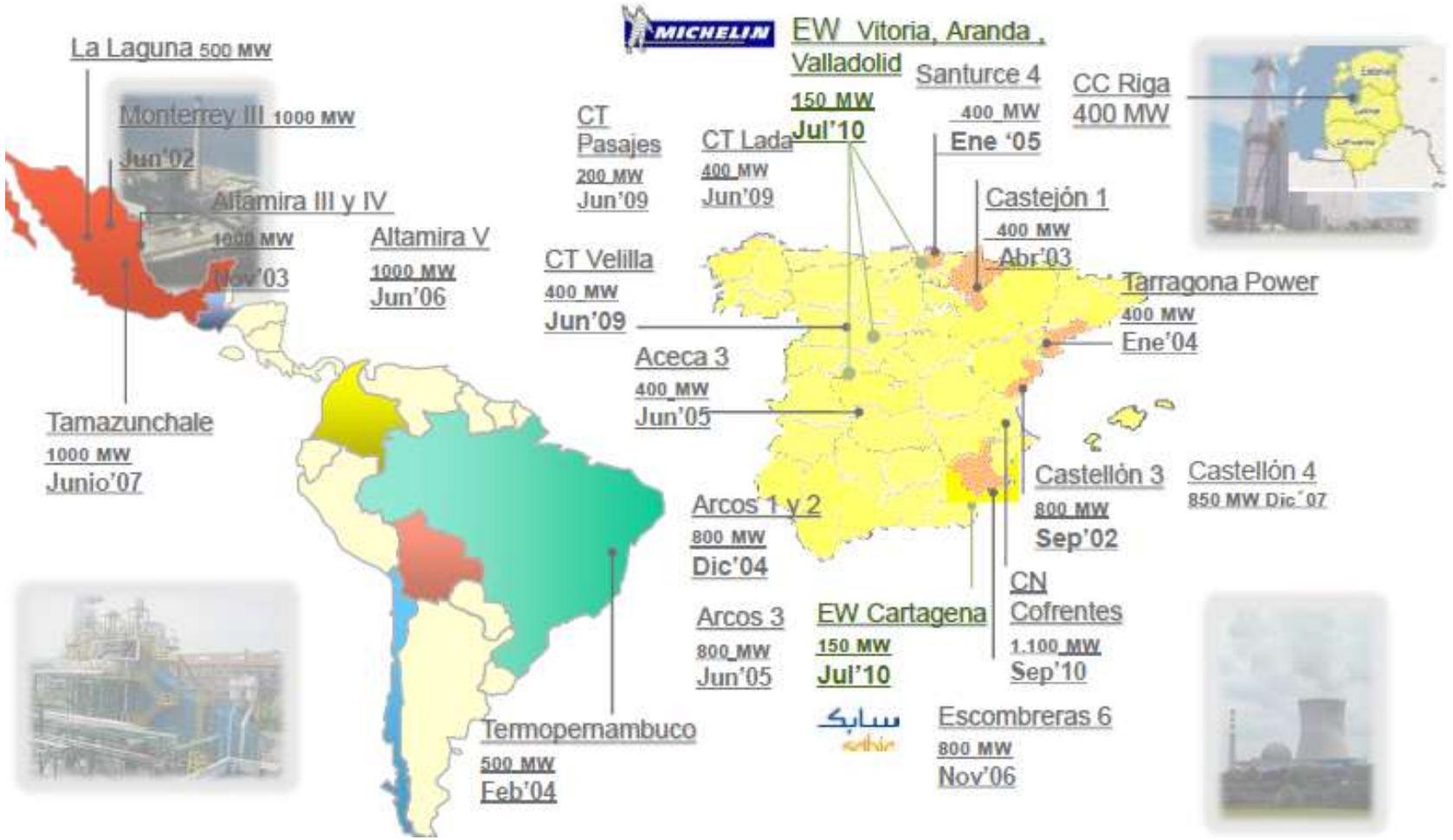


CYBERARK

CYBERARK

Контроль удалённого доступа

Iberdrola



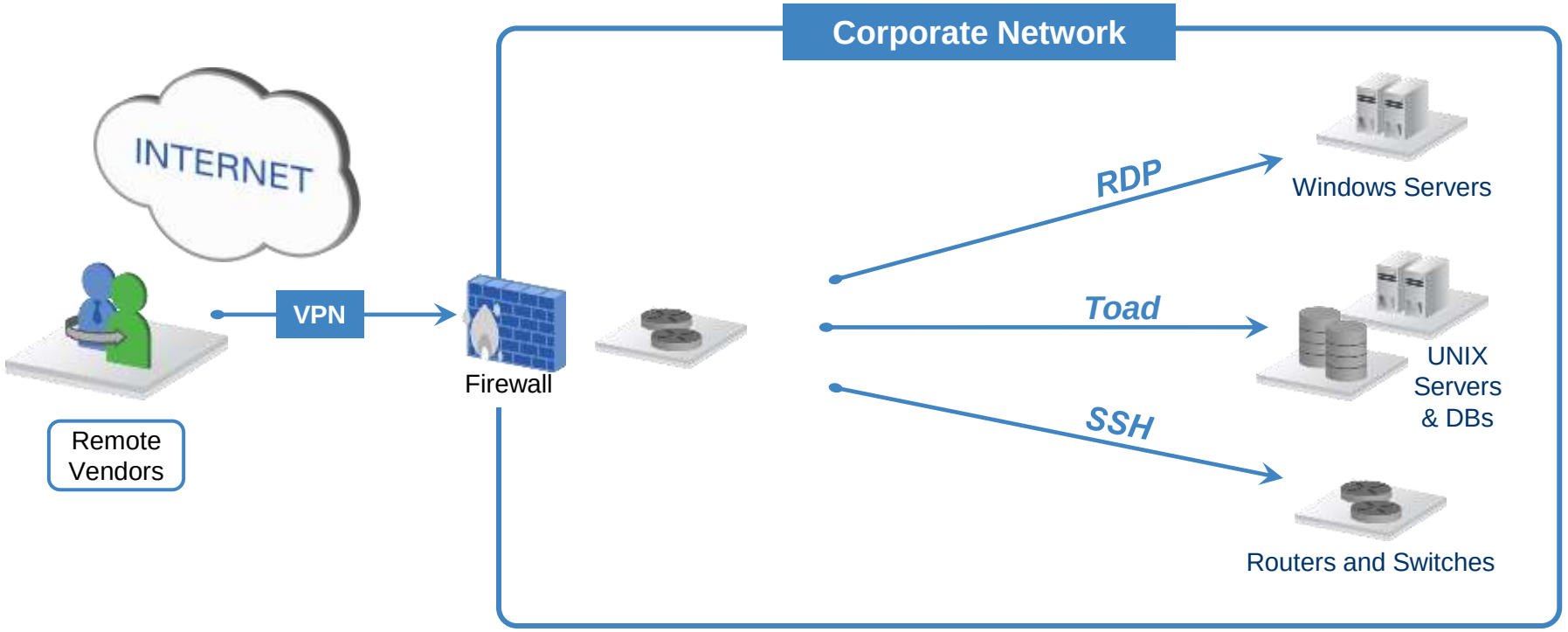
CYBERARK

Персонифицированный доступ

- Windows systems
- Unix systems
- Databases
- Network devices
- Hypervisors
- Applications
- SaaS applications
- Social media portals
- Industrial control systems

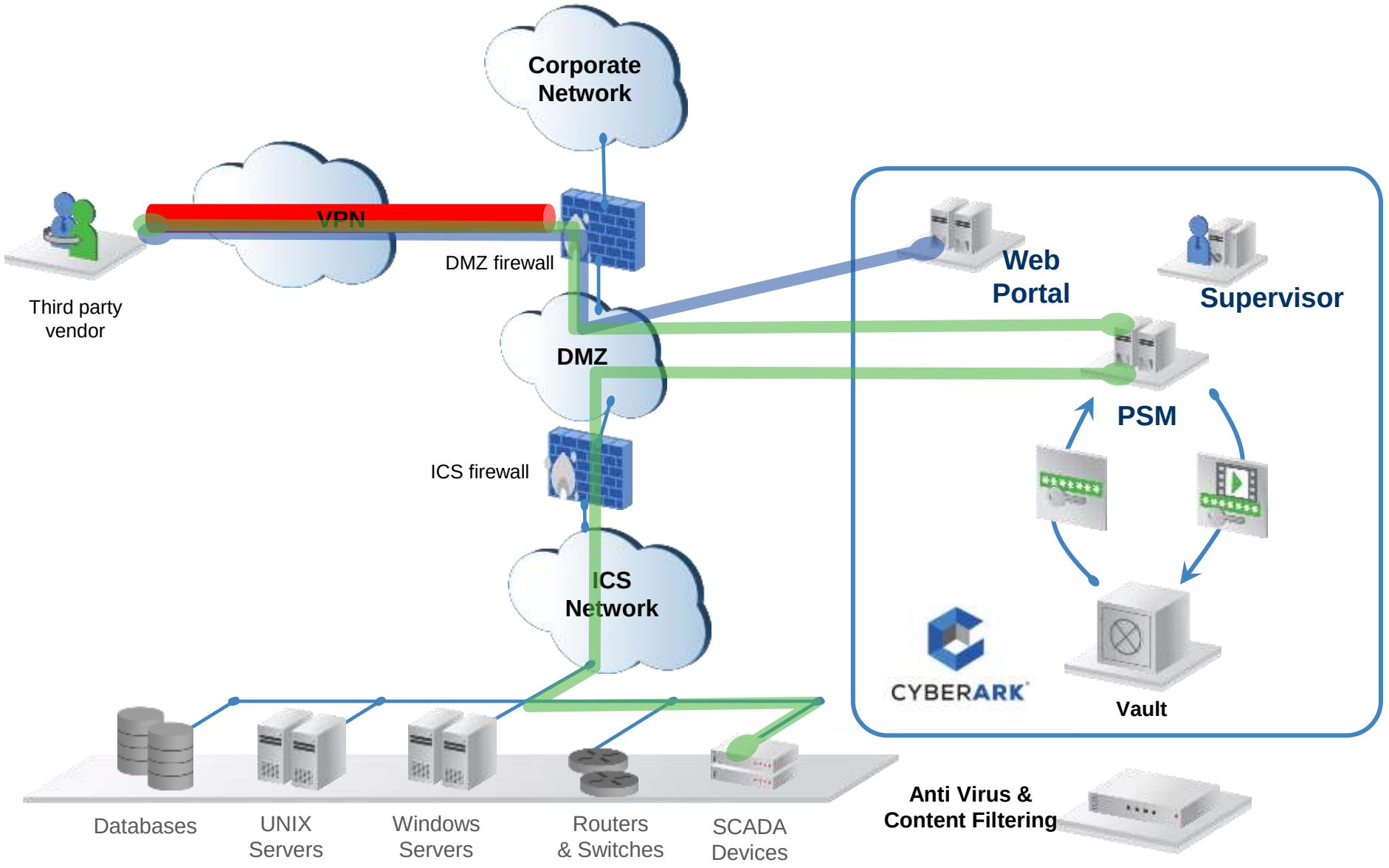
CYBERARK®

Схема доступа



CYBERARK

Защита удалённого доступа



CYBERARK

Итоги

Привилегированные аккаунты
в первой группе риска

Простого протоколирования всех действий недостаточно

CyberArk - уникальное комплексное решение проблемы
управления и защиты аккаунтов и привилегий

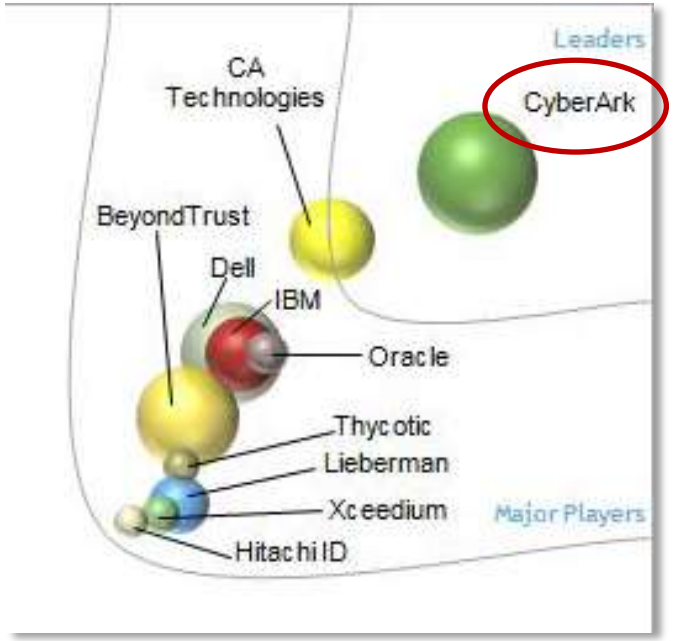
CYBERARK®

Ведущие аналитики о CyberArk

CyberArk предлагает п**олноценный спектр PAM** продуктов, которые лицензируются отдельно и поставляются в виде ПАК или АО (Gartner)

CyberArk – это «**big gorilla**» и лидер в области PAM …. Маркетинг и бизнес нацелены на решение проблем заказчиков и функционал продукта (IDC)

CyberArk Privileged Account Security установило **золотой стандарт PAM** и продолжает занимать лидирующие позиции в данной области (KuppingerCole)



Спасибо

Олег Котов
Account Executive, Russia & CIS

Mobile +7 916 836 63 68
oleg.kotov@cyberark.com
www.cyberark.com