



CYBERARK

Гигиена в цифровом пространстве. Защита аккаунтов и управление привилегиями.

Олег Котов, CISSP
Account Executive, Russia & CIS

Как страшно жить ...

Wana Decrypt0r 2.0



Payment will be

5/18/2017 16:1

Time Left

02:23:58

Your files will be

5/22/2017 16:1

Time Left

06:23:58

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Tactics, techniques and procedures of financial attacks attributed to the Lazarus group

Lazarus is widely considered including the \$81 million he and several other attacks ag hackers follow a set of tactic penetrate targeted systems

Step 1

Compromise of a webserver



OR



2. The exploit is placed on the hacked website with a whitelist of targets to serve the exploit to

3. The target visits a government website and becomes infected

While investigating Lazarus' fir malware samples related to reo Kaspersky Lab products succes

KIM ZETTER SECURITY 03.03.18 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattiaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

T message filtering are is integrated te rogue messages ed by the attackers



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



**Компрометированные
учётные данные**



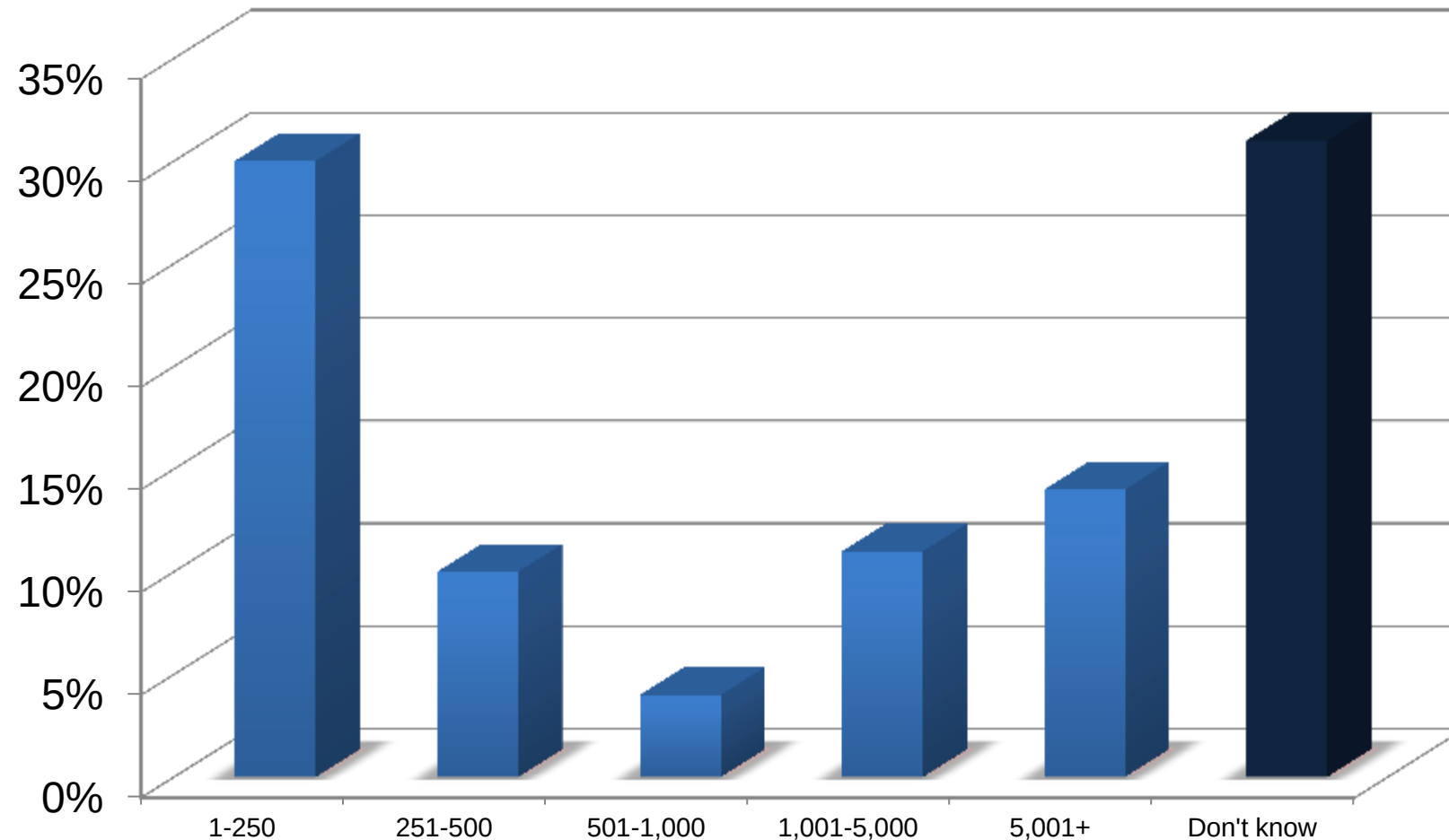
Возможности злоумышленника:

- Обходить системы безопасности и мониторинга
- Получать доступ к любой информации на любом устройстве
- Остановить бизнес-процессы
- Нанести физический ущерб



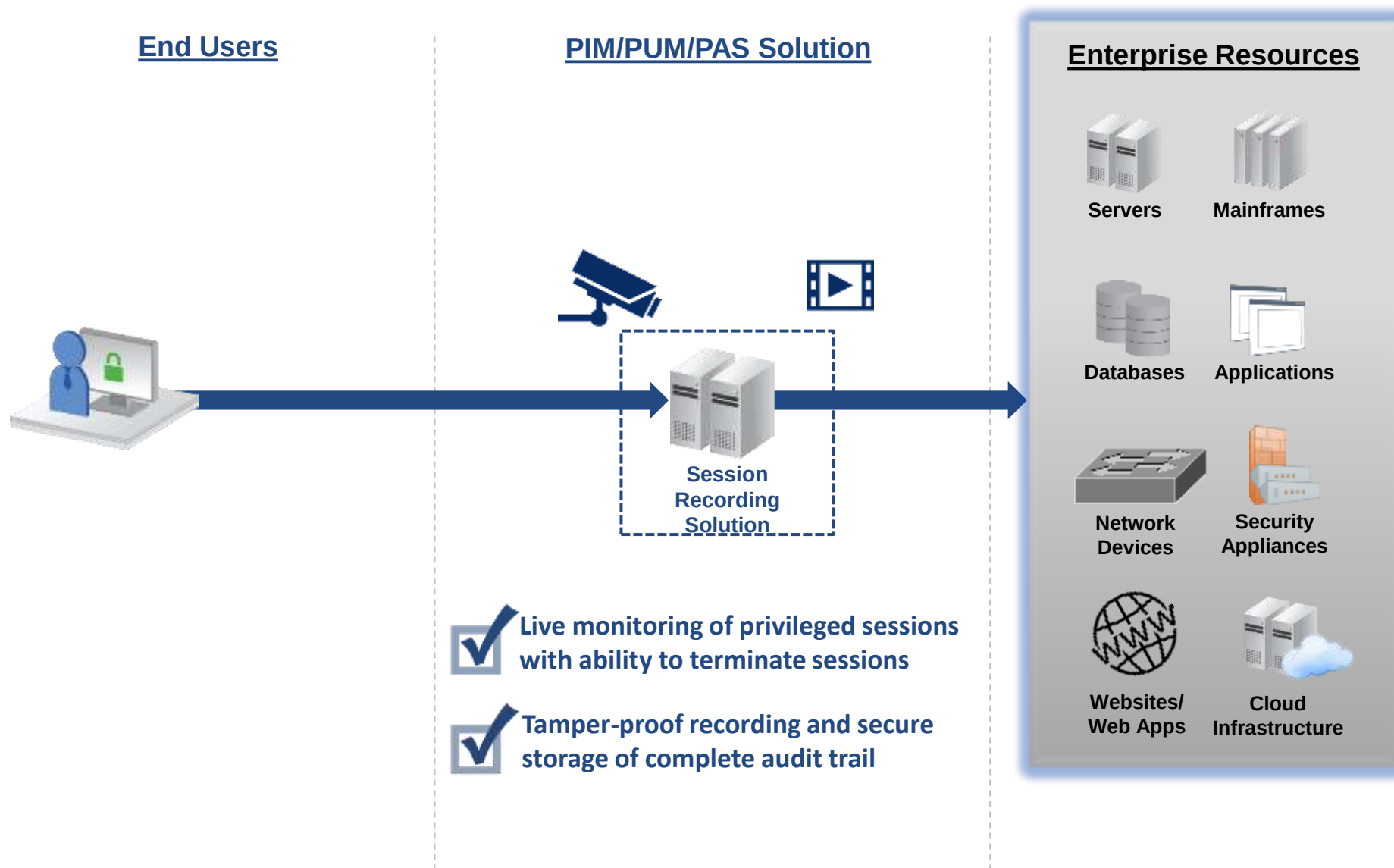
CYBERARK®

Сколько привилегированных аккаунтов у вас?

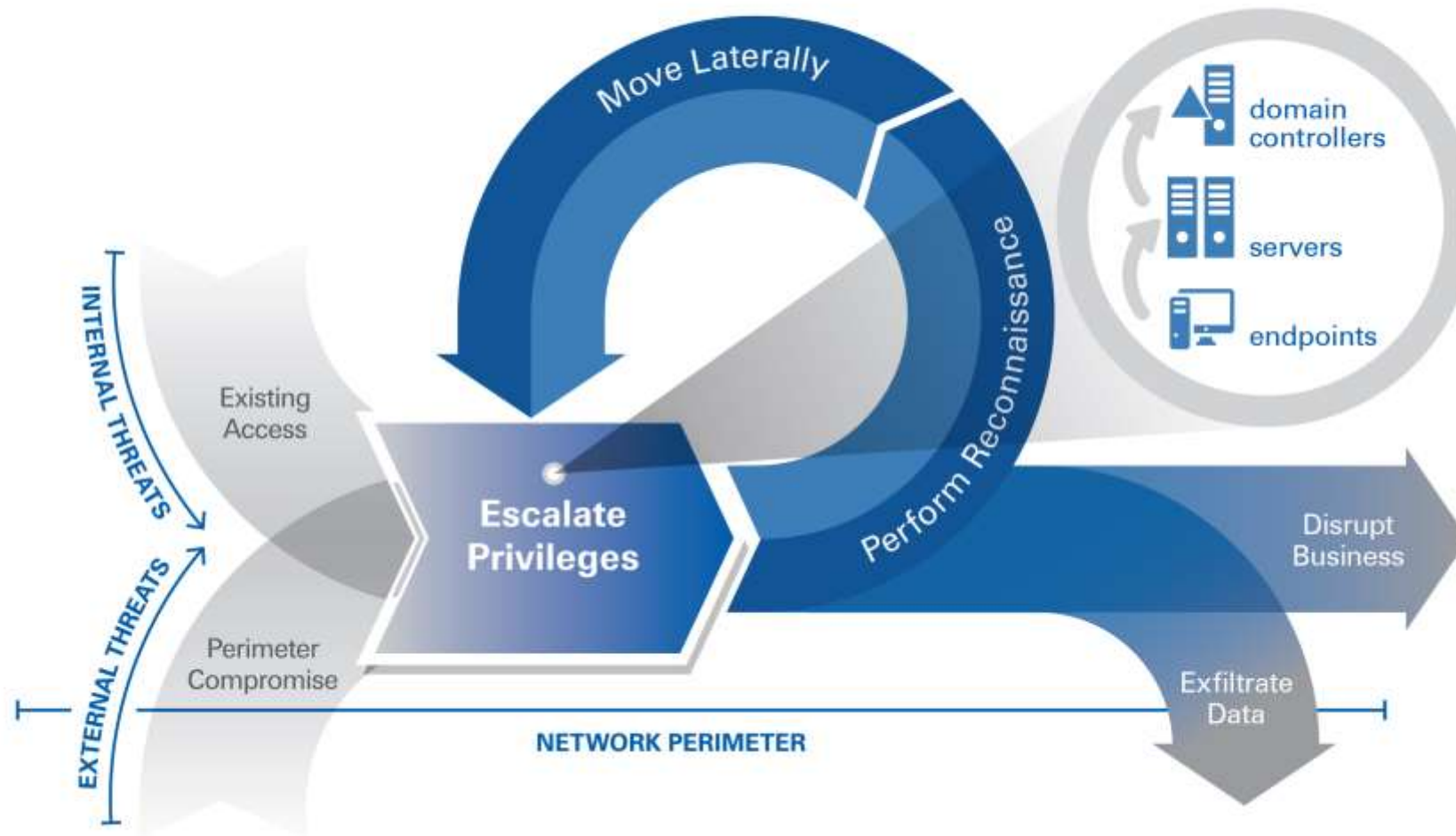


Cyber-Privileged Account Security & Compliance Survey, May 2015 (Enterprise > 5000 Employees)

Классический подход защиты привилегированного доступа



Полная картина



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 Privileged Account Security

Core Privileged Account Security



Enterprise Password Vault®



Privileged Session Manager®



Privileged Threat Analytics

Credential protection, Session Isolation and Monitoring,
Privileged Analytics and Threat Detection

Least Privilege Control for *NIX and Windows Servers
and Domain Controller Protection



App Identity Manager
/ Conjur

DevOps & Apps
Secrets Management



Endpoint Privilege
Manager

Endpoint Least Privilege,
App Control & Credential
Theft Protection



On-Premises



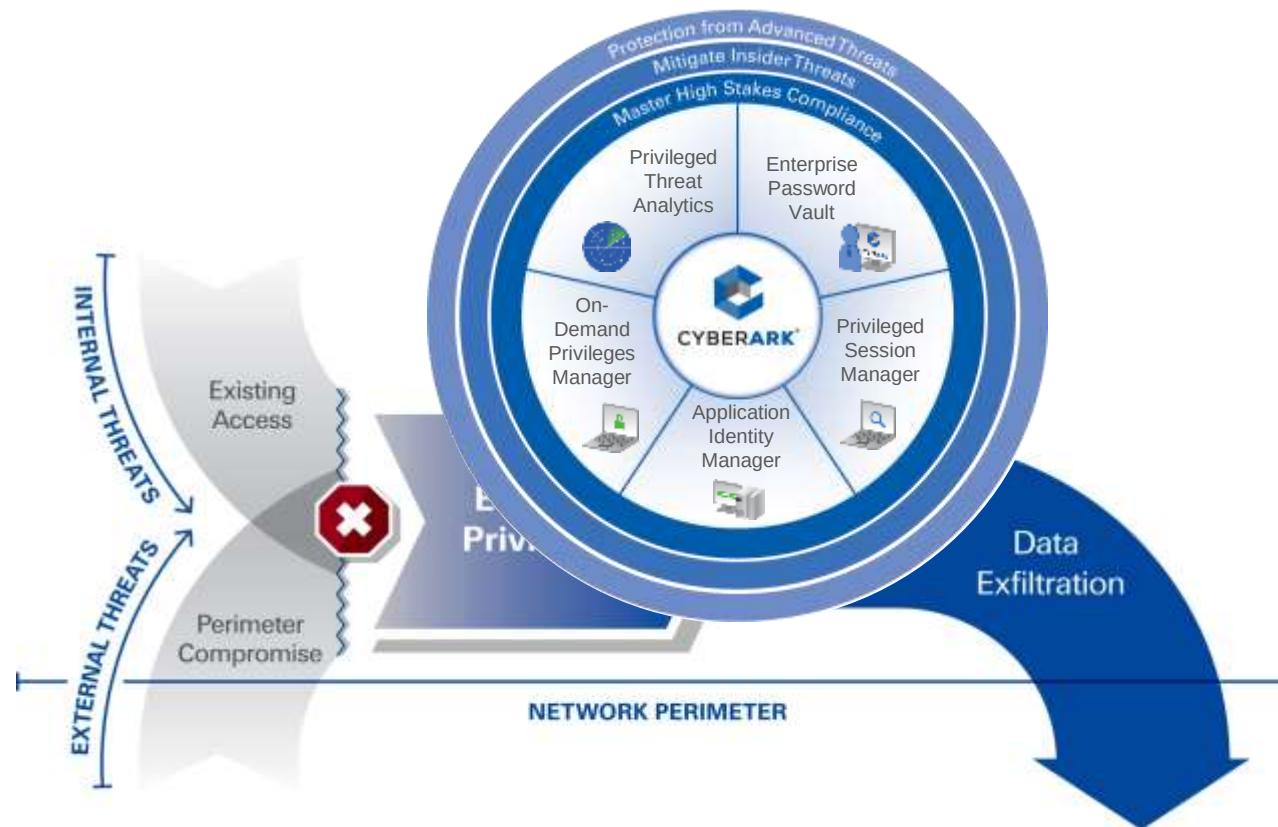
Hybrid



Cloud



Комплексный подход

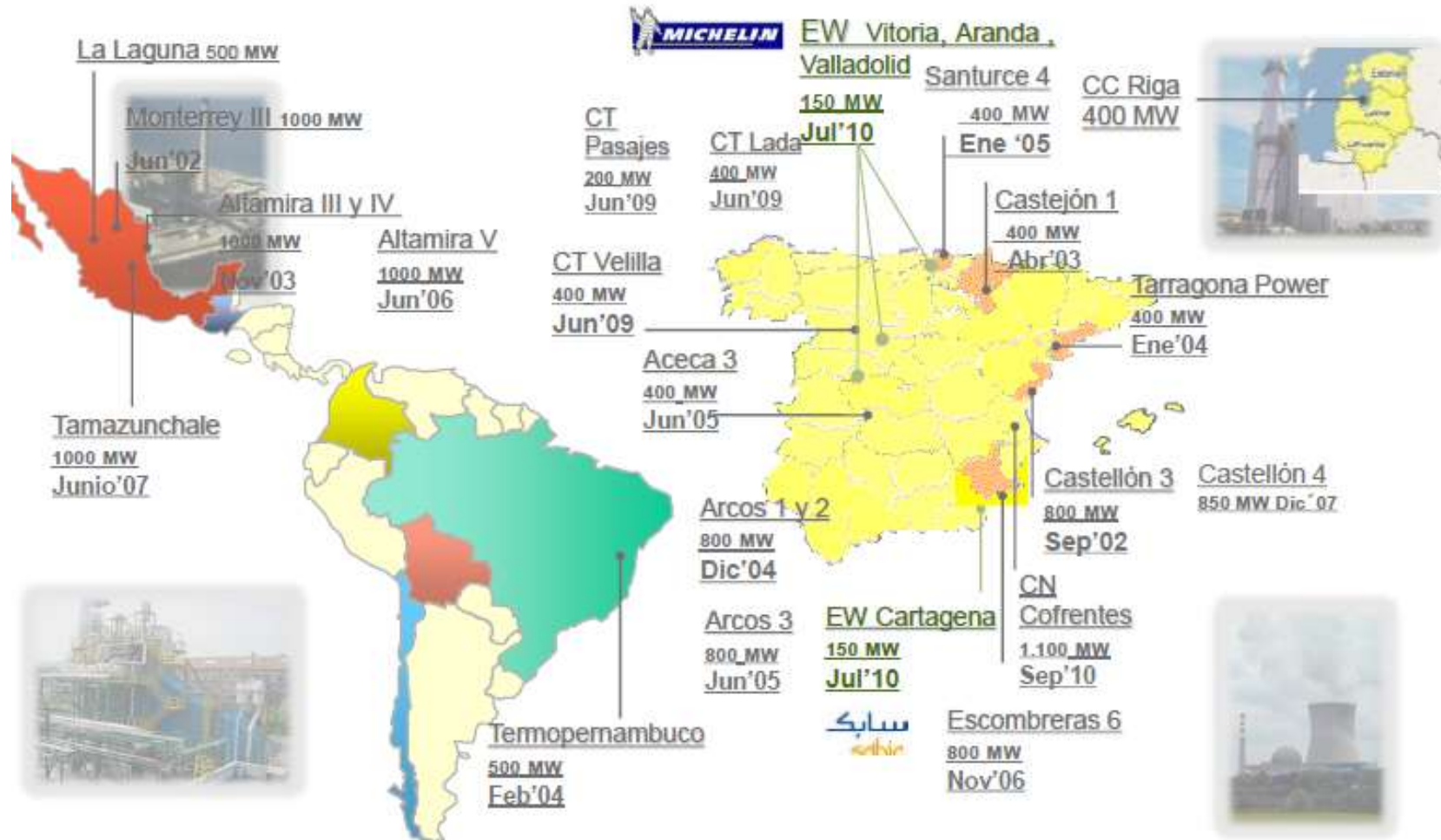




CYBERARK



Контроль удалённого доступа

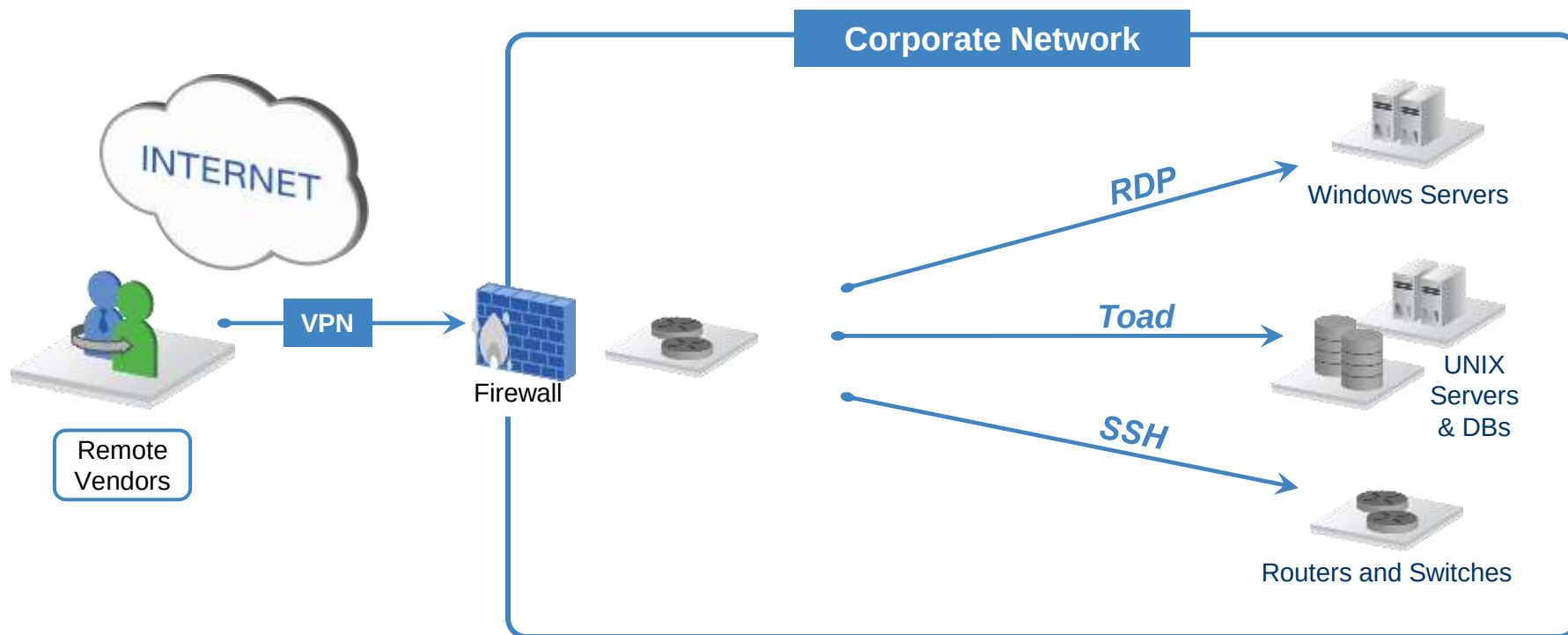


Персонализированный доступ

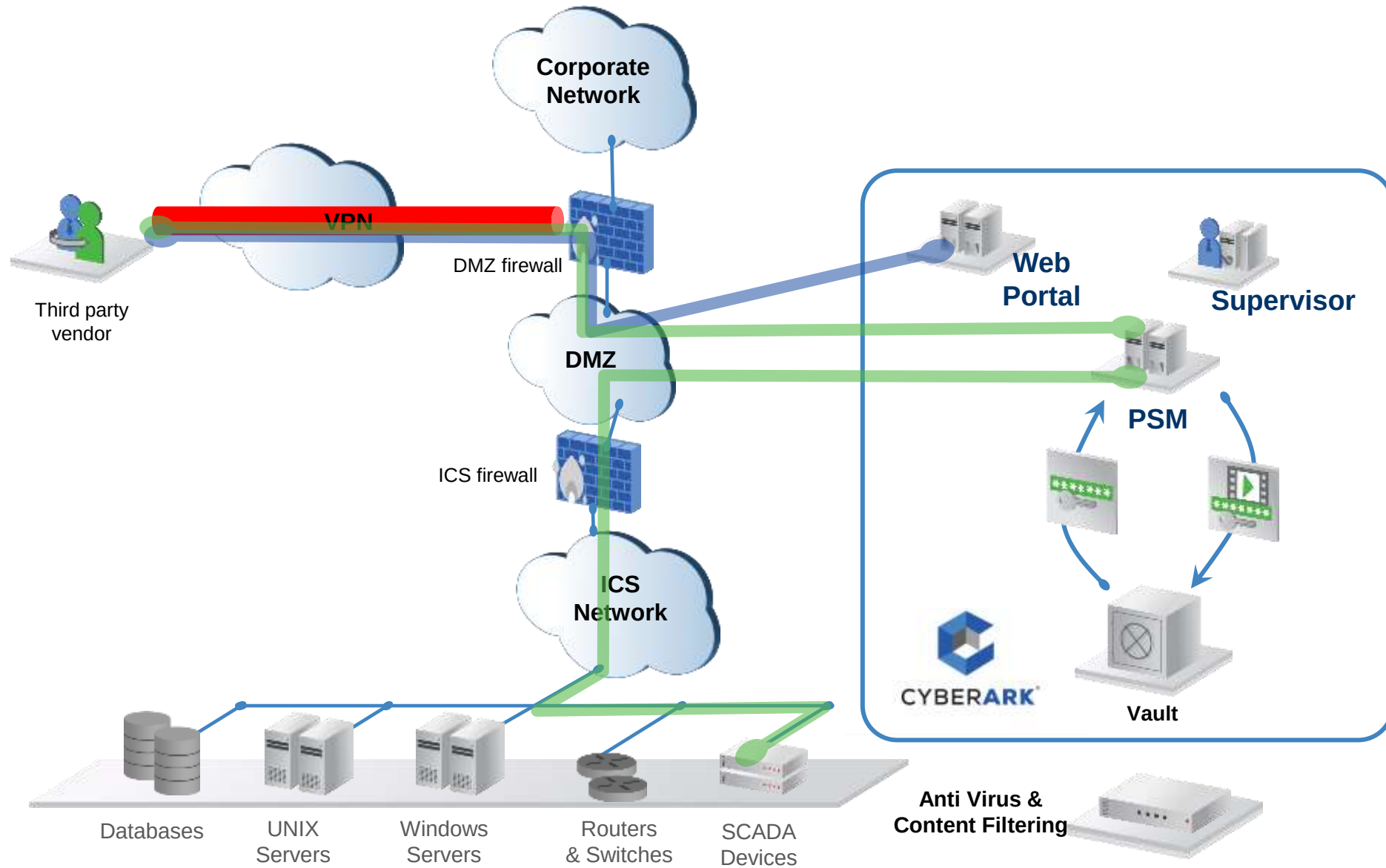


- Windows systems
- Unix systems
- Databases
- Network devices
- Hypervisors
- Applications
- SaaS applications
- Social media portals
- Industrial control systems

Схема доступа



Защита удалённого доступа



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

Gartner

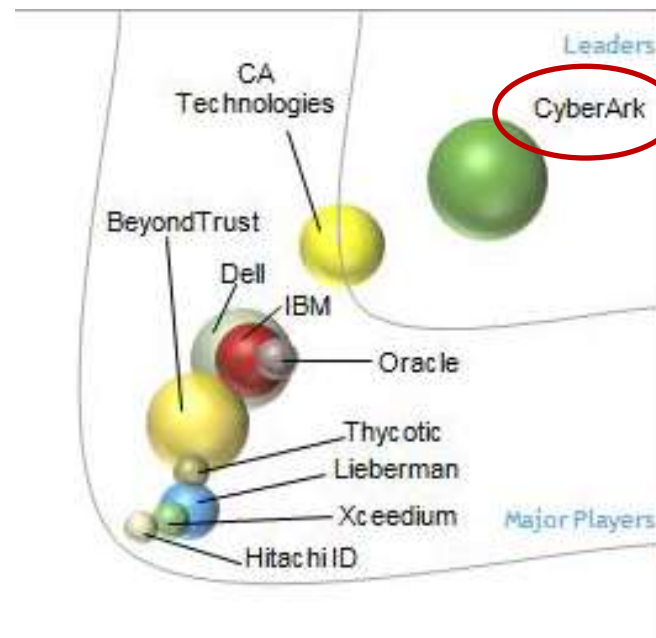
CyberArk предлагает **полноценный спектр PAM** продуктов, которые лицензируются отдельно и поставляются в виде ПАК или АО (Gartner)

IDC
Analyze the Future

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

kuppingercole
ANALYSTS

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