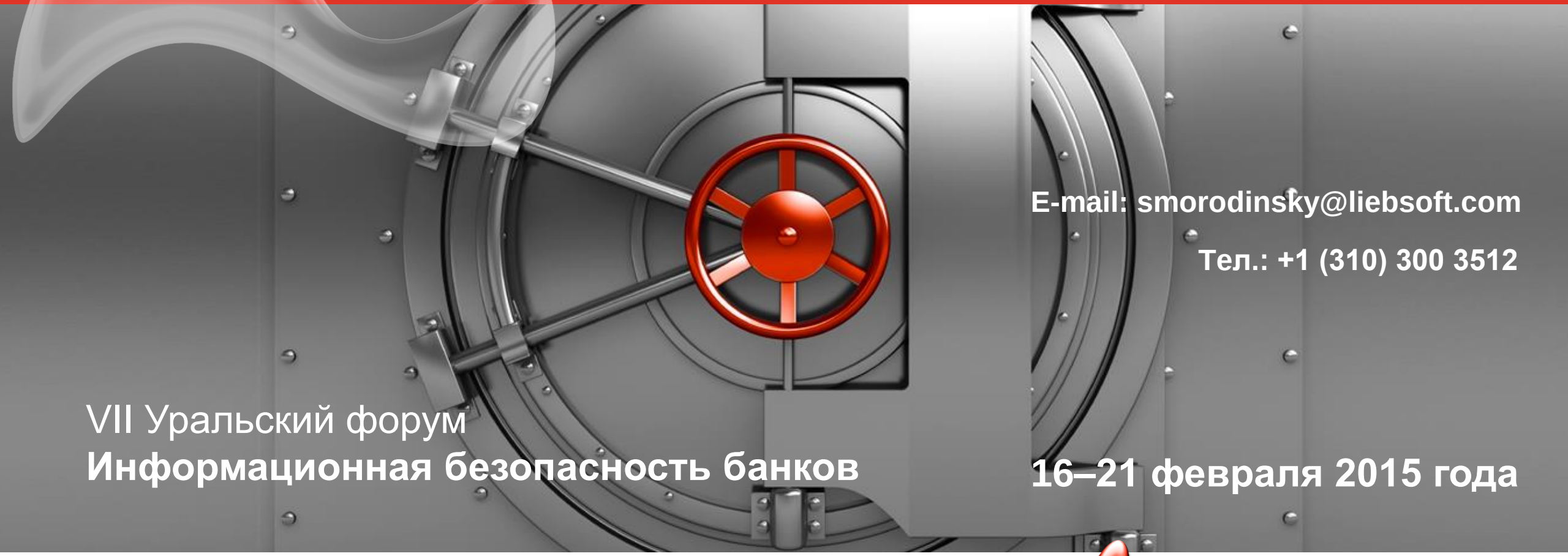
Автоматизированное Управление Привилегированным Доступом: Эволюция Управления Паролями или Новая Парадигма?

Лев Смородинский, вице-президент по развитию бизнеса в Восточной Европе,
Lieberman Software Corporation



E-mail: smorodinsky@liebsoft.com

Тел.: +1 (310) 300 3512

VII Уральский форум
Информационная безопасность банков

16–21 февраля 2015 года

LIEBERMANSOFTWARE™

Содержание

Немного истории: От первого пароля до атаки с 80 млн украденными персональными записями

Почему привилегированные записи цель всех атак?

Защита периметра не спасает привилегированные «учётки»

Как минимизировать последствия компрометации?

Lieberman Software ERPM – автоматизированное управление привилегиями

Содержание

Немного истории: От первого пароля до атаки с 80 млн украденными персональными записями

Почему привилегированные записи цель всех атак?

Защита периметра не спасает привилегированные «учётки»

Как минимизировать последствия компрометации?

Lieberman Software ERPM – автоматизированное управление привилегиями

От любопытства и любви к компьютерам до преступления!

- Первый компьютерный пароль использовался в 1961 г. в МТИ (MIT) в год полёта в космос Юрия Гагарина
- Первые компьютерные преступления:
  - В 1983 году Кевин Митник в 20 лет взломал компьютер в Пентагоне
  - В 1988 Роберт Моррис в 23 года создал первый сетевой червь, парализовавший 6000 компьютеров и вызвавший $ 50,000 убытков
  - В 1994 году Владимир Левин вторгся в компьютер американского банка (Citibank) и украл $10M
  - В 1999 Джонатан Джеймс в 16 лет проник в компьютер NASA и получил доступ к данным на сумму $1,7M

От юных хакеров-одиночек до кибервойн

- Летом 2010 года, обнаружено первое проникновение вредоносного ПО под названием Stuxnet в заводские компьютеры, которое распространилось по заводам всего мира.

- Последние «жертвы» и некоторые последствия:
  - Target Corp. (ритейлер) – по крайней мере 40 млн кредитных карт похищено (в 4 кв. 2013 Target потратил $146 млн на восстановление)
  - Home Dupot (ритейлер) – 56 млн кредитных карт в опасности
  - JP Morgan (банк) - генеральный директор JP Morgan пообещал, что к концу 2014 года, банк будет тратить $250 млн в год в области кибер безопасности и использовать 1000 сотрудников (скомпрометировано 76 млн клиентов и 7 млн бизнесов)
  - Apple (электроника и онлайн-сервисы) – акции упали на 4.22%

Каждую неделю новые заголовки

Anthem Data Breach hits 80 million

Anthem – вторая в США по величине компания: предоставляющая медицинские страховки

- Сообщение 4-ого февраля 2015 г.: хакеры украли персональную информацию о более, чем 80 миллионах клиентов, что сделало это крупнейшим взломом данных

26 ?

“Это просто …”

Шансы велики, что Ваша инфраструктура уже нарушена, но Вы об этом ещё не знаете!

- **97% организаций** были в той или иной степени взломаны
- **67%** пострадавших компаний были **уведомлены третьими лицами**
- **Партнеры и клиенты** часто первыми узнают о ваших проблемах

FireEye / Mandiant 2014

Взломы инфраструктуры часто не лобовые атаки

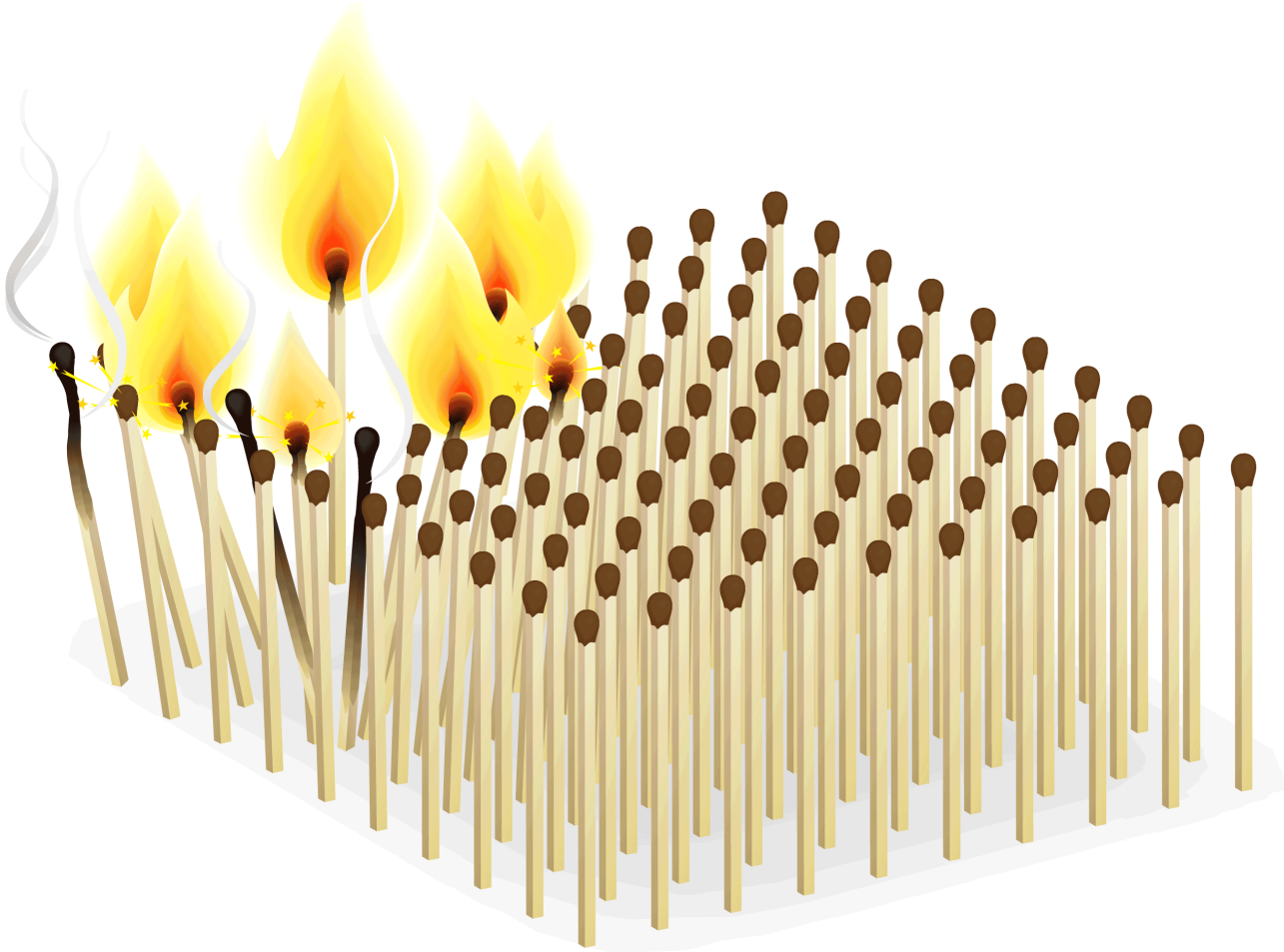
Атакующие подолгу гнездятся во взломанной сети, прежде чем начать атаку

- **229 дней** является средним временем до обнаружения атаки
- Хакеры находились в сети Home Depot в течение **почти 5 месяцев**, прежде чем были обнаружили.

Mandiant Threat Report / KrebsOnSecurity

Анатомия развития атаки

- **Начинается с одной точки уязвимости**
- Прорыв быстро распространяется, используя **слабые методы защиты привилегированных учетных записей**



Последствия не заставляют ждать…

51% клиентов переносят свой бизнес в другое место после нарушения.

Infosecurity Magazine, September 2014

Содержание

Немного истории: От первого пароля до атаки с 80 млн украденными персональными записями

Почему привилегированные записи цель всех атак?

Защита периметра не спасает привилегированные «учётки»

Как минимизировать последствия компрометации?

Lieberman Software ERPM – автоматизированное управление привилегиями

Атакующие извне должны получить полномочия внутренних привилегированных пользователей

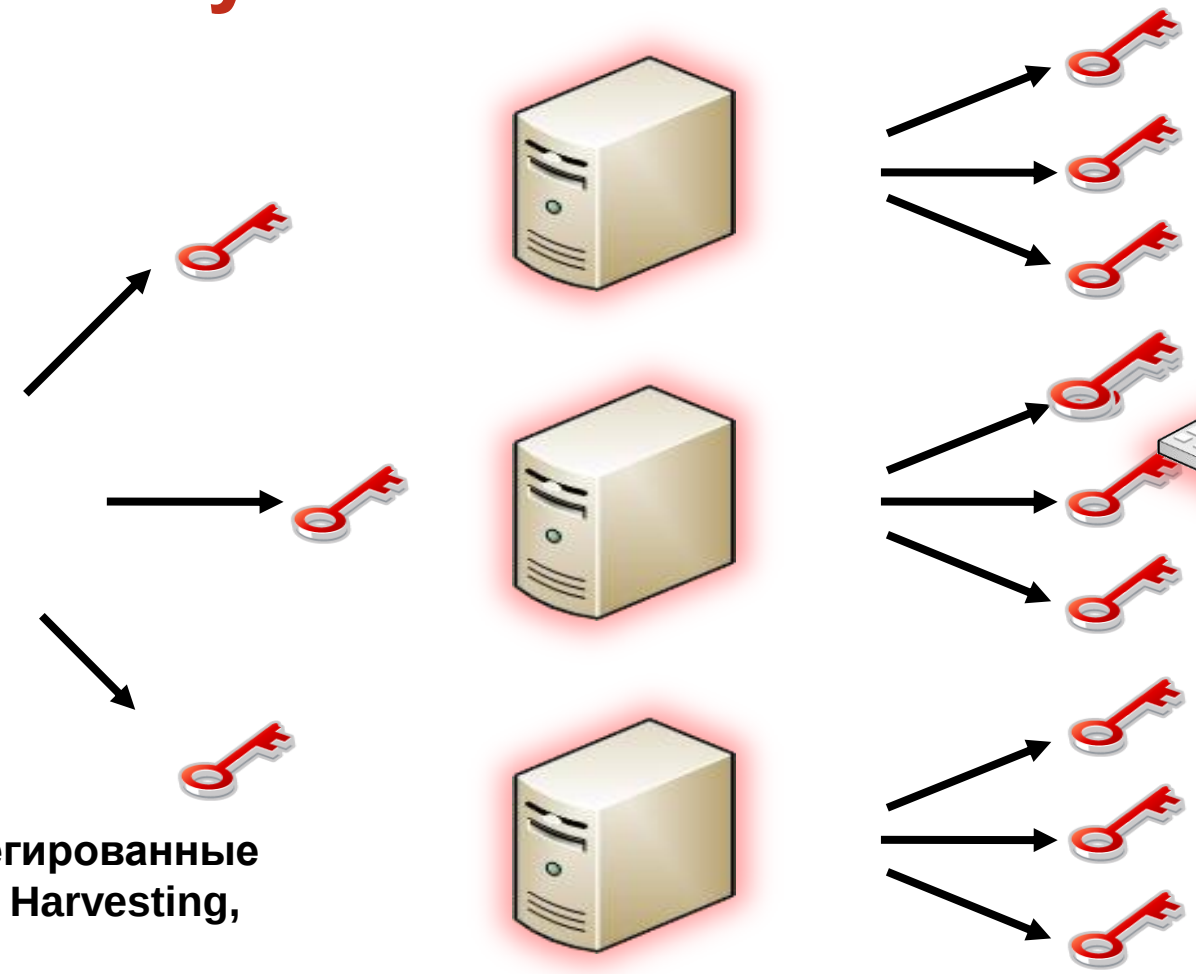
Mandiant M-Trends 2014 Report

Привилегированный доступ необходим для успешной кибератаки

Разведка	Сканирование	Доступ и Эскалация	Эксфильтрация данных	Поддержание	Нападение	Скрытие следов
• *Maltego* • *Metagoofil* • *ExifTool*	• *NMAP* • *Nessus* • *Shodan*	• *THC-Hydra* • *Rainbow Table* • *John the Ripper* • *Metasploit*	• *Corkscrew* • *OpenPuff* • *Sabznameh*	• *Linux identities* • *Windows identities*	• *Flashrom*	• *Bitblinder* • *Tor*

Каждый из этих этапов требует знания привилегированных учётных записей

Атаки распространяются через неуправляемых привилегированные учетные записи

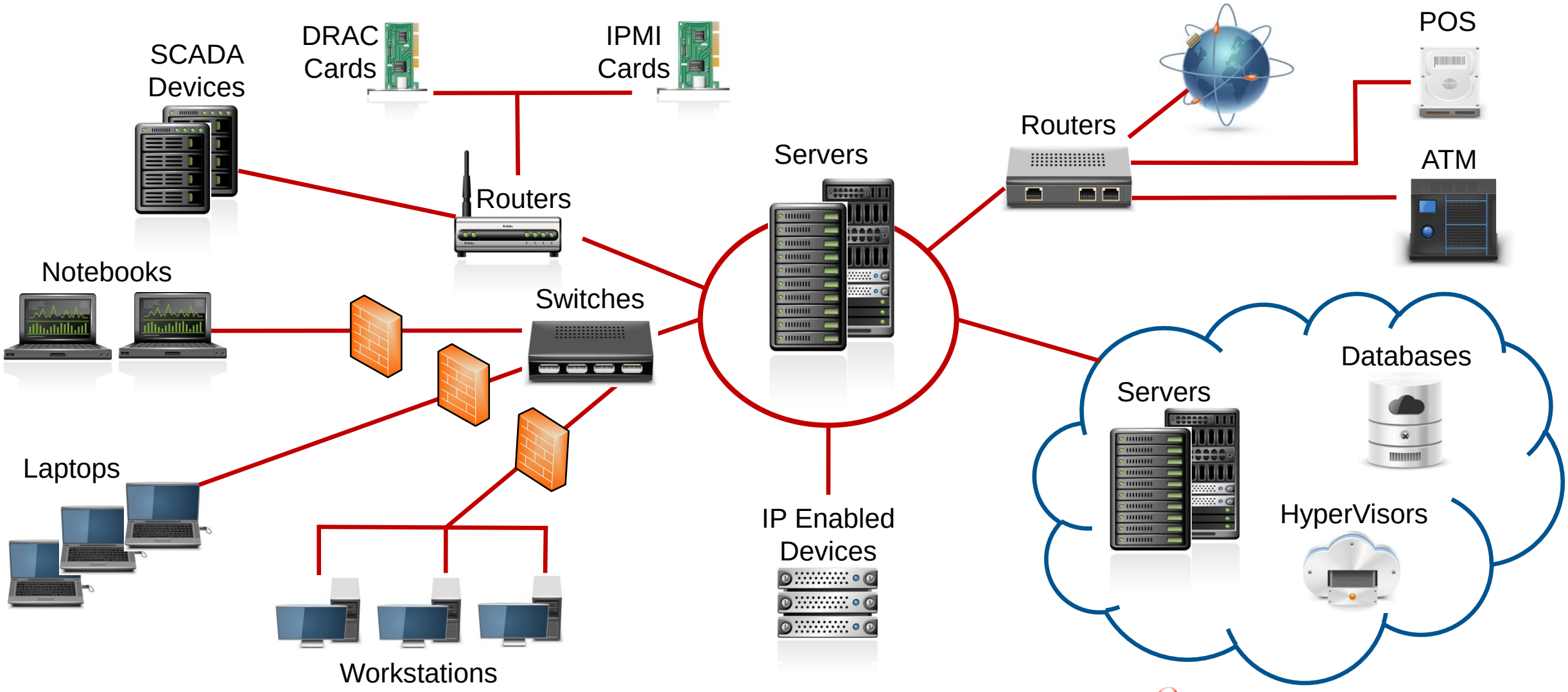


Скомпрометированные системы

ПО злоумышленников прыгает от системы к системе, используя неуправляемые привилегированные учетные записи

Общие и слабые привилегированные пароли учетных записей, Harvesting, Key Logging

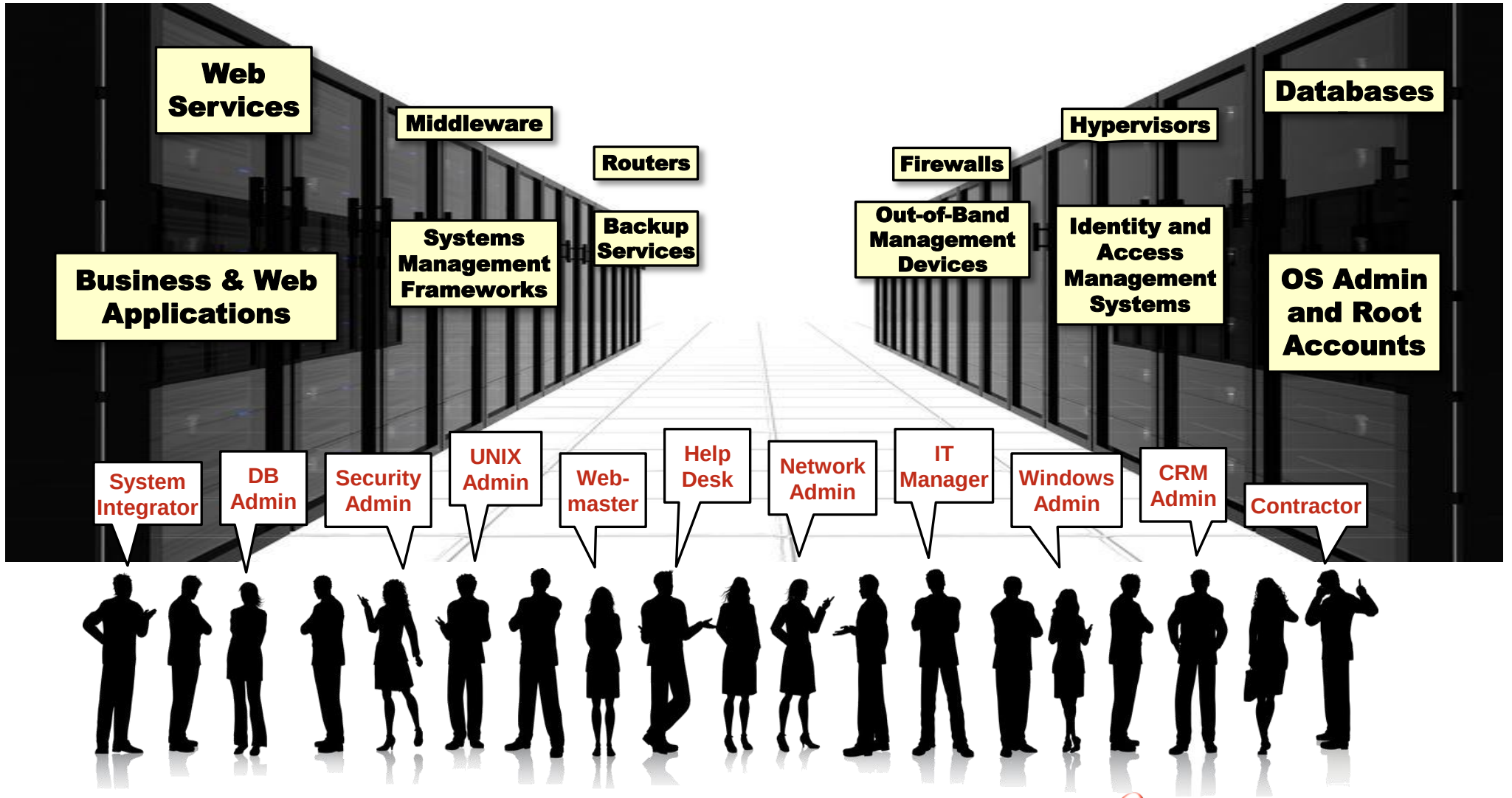
Вездесущность уязвимостей 1: аппаратура



Вездесущность уязвимостей 2: ПО

- Windows Service Accounts
- Windows Scheduler Task RunAs Identities
- Windows Scheduler At Service Accounts
- COM+ Application Identities
- DCOM Object RunAs Identities
- IIS6 Metabase Account Info
- IIS7 Account Info
- SCOM RunAs Accounts
- Accounts in .NET Config
- Credentials in SQL Server
- String Replacements
- SharePoint
- Logon Cache
- Auto Logon Account
- Local Cache JAVA Client
- SQL Reporting Services
- SSH Keys
- IBM WebSphere, Oracle WebLogic
- Twitter, Facebook, LinkedIn, etc.
- IBM, Oracle, SAP, others…

Вездесущность уязвимостей 3: персонал



Содержание

Немного истории: От первого пароля до атаки с 80 млн украденными персональными записями

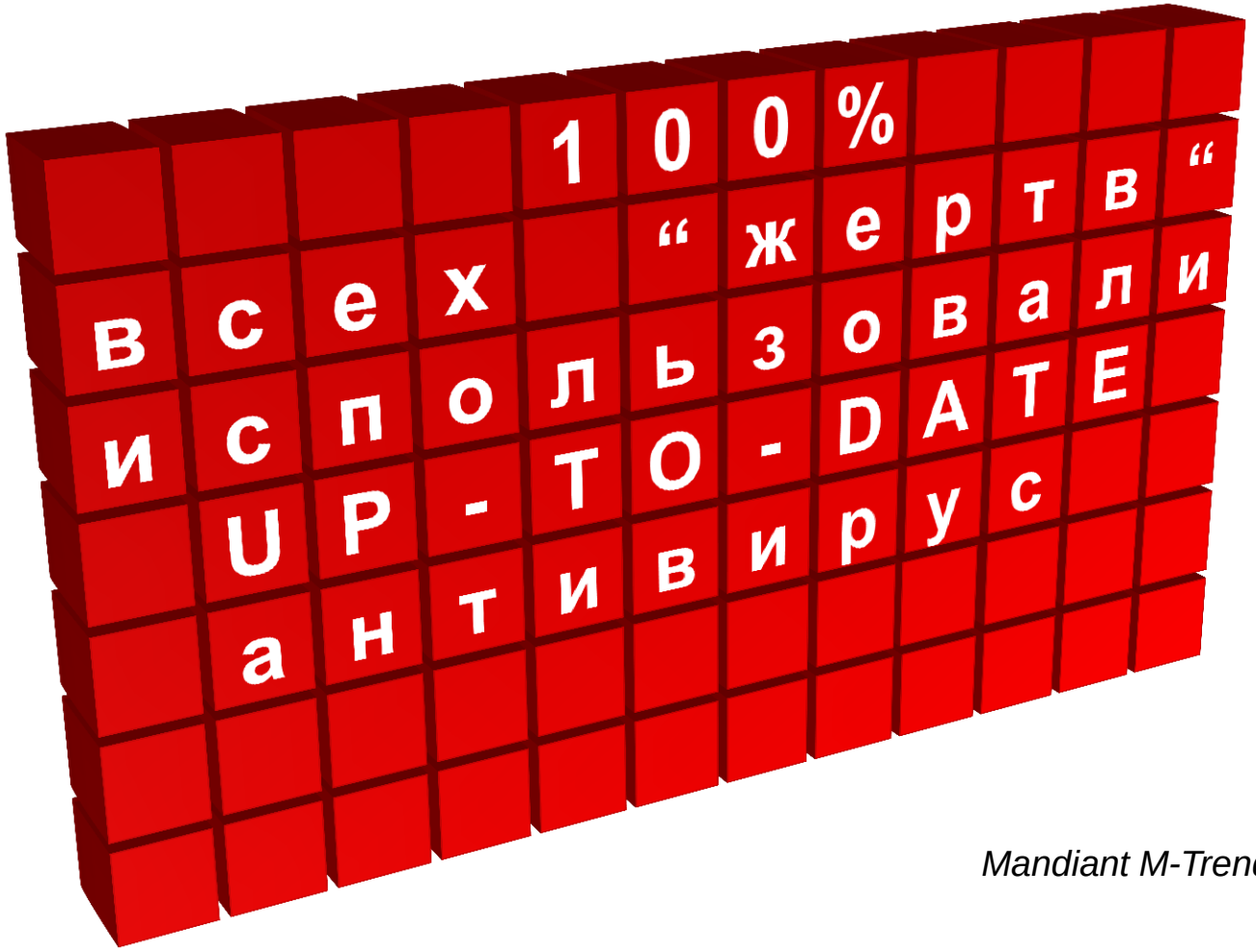
Почему привилегированные записи цель всех атак?

Защита периметра не спасает привилегированные «учётки»

Как минимизировать последствия компрометации?

Lieberman Software ERPM – автоматизированное управление привилегиями

Атакующие прорвутся внутрь периметра сети

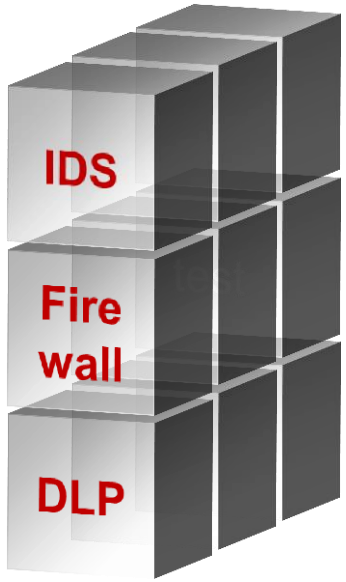


Mandiant M-Trends 2014 Report

Защита периметра не спасает от внутренних угроз

Взлом данных начинается и происходит внутри сети

Защита периметра



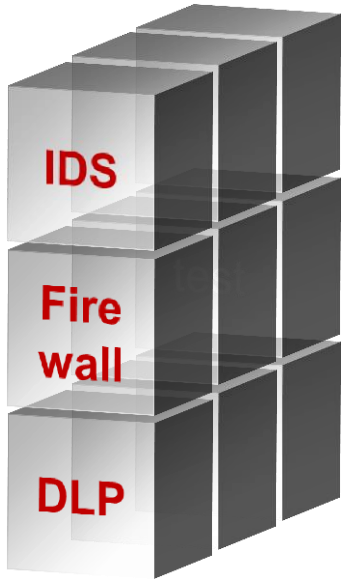
- 18% нарушений данных в 2013 из-за действий инсайдеров
- 88% инсайдерских инцидентов, вызванно злоупотреблением привилегированного доступа

Эдвард Сноуден, рекламный пример угрозы инсайдер

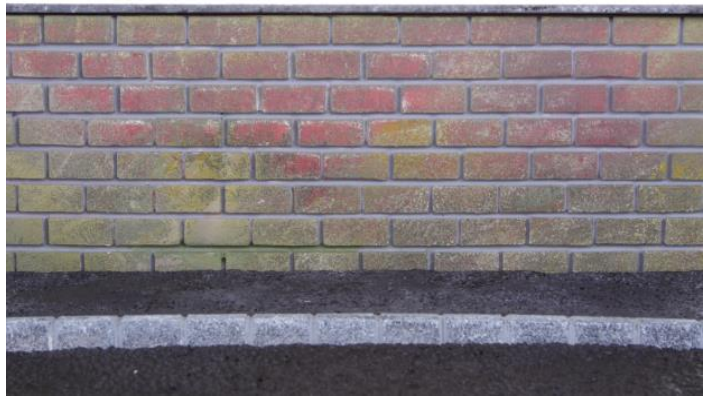
Verizon 2014 Data Breach Investigations Report

Защита периметра не достаточно гибка

Защита периметра



- Отвечает только после обнаружения угрозы
- Не может остановить распространение атаки



Уязвимость IT Аутсорсеров

Когда аутсорсеры становятся привилегированными инсайдерами

- **Target**: атака началась с поставщика HVAC
- **NSA**: Edward Snowden, контрактор компании Booz Allen Hamilton
- *После окончания котракта привилегированный доступ не отменяется.*

"Крупные организации часто не разглашают о данные о нарушениях поставщиков и субподрядчиков ".

Wall Street Journal, 9/18/14

"Chinese Hacked U.S. Military Contractors, Senate Panel Say"

Содержание

Немного истории: От первого пароля до атаки с 80 млн украденными персональными записями

Почему привилегированные записи цель всех атак?

Защита периметра не спасает привилегированные «учётки»

Как минимизировать последствия компрометации?

Lieberman Software ERPM – автоматизированное управление привилегиями

Позади брандмауэра: управление привилегиями

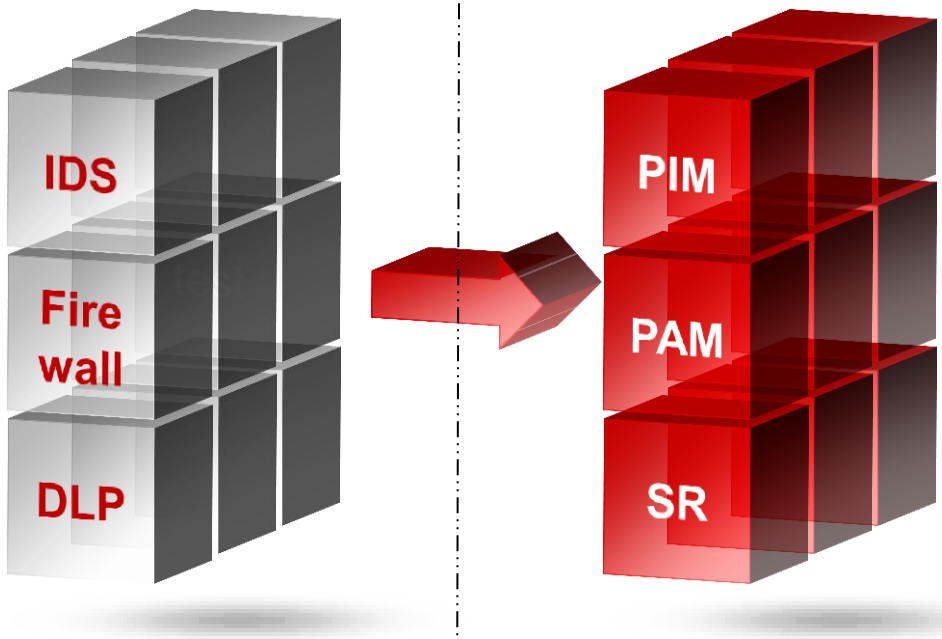
Когда защита периметра не выручает, работает управление привилегиями

Защита периметра

Внутренняя защита

Detect and Respond

Обнаружить и Ответить



Privileged Identity Management (PIM)

Privileged Access Management (PAM)

Session Recording (SR)

Управление привилегиями

Proactive Continuous Counteraction

Проактивное Непрерывное Противодействие

Автоматизированное управление привилегированным доступом

Аудит — Видео и текстовый аудит

Управление приложениями — Настройка и запуск приложений

Уполномочивание — Настройка полномочий пользователей

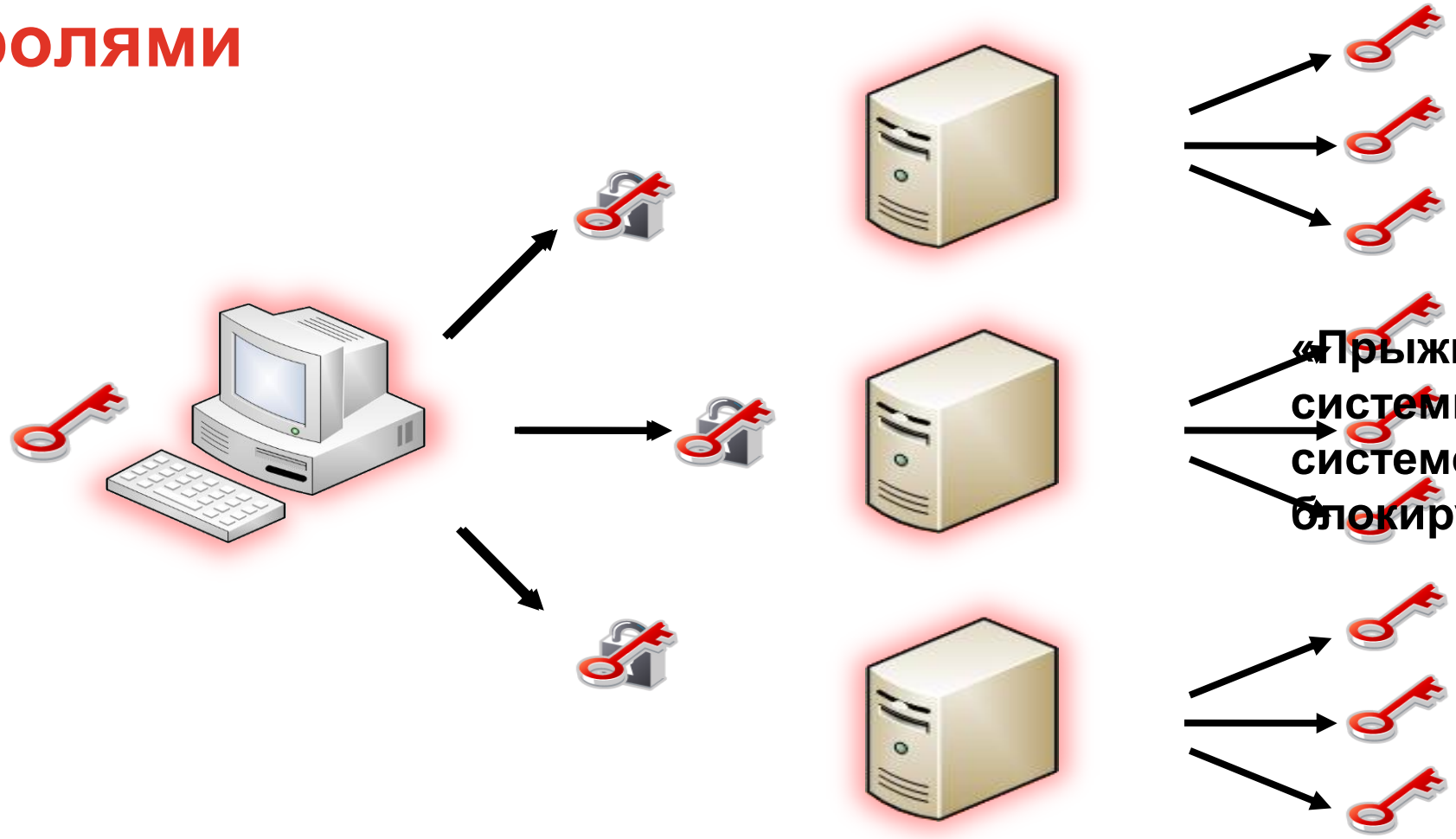
Противодействие — Часто меняющиеся криптографически сложные пароли

Обнаружение — Привилегированные аккаунты и их использование

1. ОБНАРУЖЕНИЕ: автоматическое, повторяющееся быстрое и полное

- Выявление и документирование критических ИТ-активов, их изменений, привилегированных учетных записей и их взаимозависимости
- Атакующие найдут любую уязвимость
- Все подсоединенные к сети системы и устройства должны быть под управлением

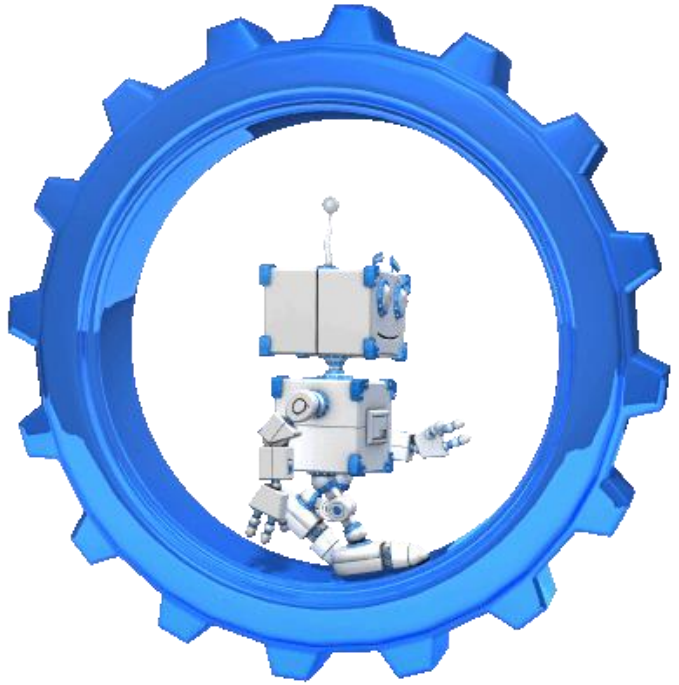
ПРОТИВОДЕЙСТВИЕ: распространение атаки останавливается уникальными, часто меняющимися паролями

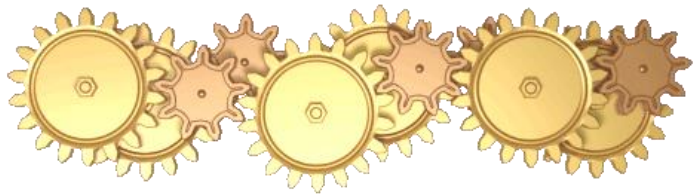


«Прыжки» от системы к системе блокируются

ПРОТИВОДЕЙСТВИЕ: гнездование становится бесполезным

- Управляемое время жизни паролей ограничивает значимость потерь от взломанных учетных записей
- Масштабируемость и автоматизация позволяют изменять учетные данные ежедневно и даже ежечасно
- Ваши оппоненты автоматизированы. Вы должны быть автоматизированы тоже.





Делегирование, Управление приложениями, Аудит

- Делегирование доступа к привилегированным аккаунтам для реализации минимальных привилегий
- Настройка доступа к приложениям
- Защищённый запуск приложений через бастион сервер с видео и текст аудитом

Оркестровка безопасности

- Комплекс организационно-технических мероприятий под руководством дирижёра:
  - CEO – «дирижёр», CISO – «первая скрипка»
- Архитектура:
  - Автоматизация – исключение человеческого фактора
  - Масштабируемость – сотни тысяч компьютеров (замена 1000 паролей в минуту)
  - Высокая доступность (избыточность всех компонентов архитектуры)
  - Защищенная среда администрирования с видео и текстовым аудитом

Содержание

Немного истории: От первого пароля до атаки с 80 млн украденными персональными записями

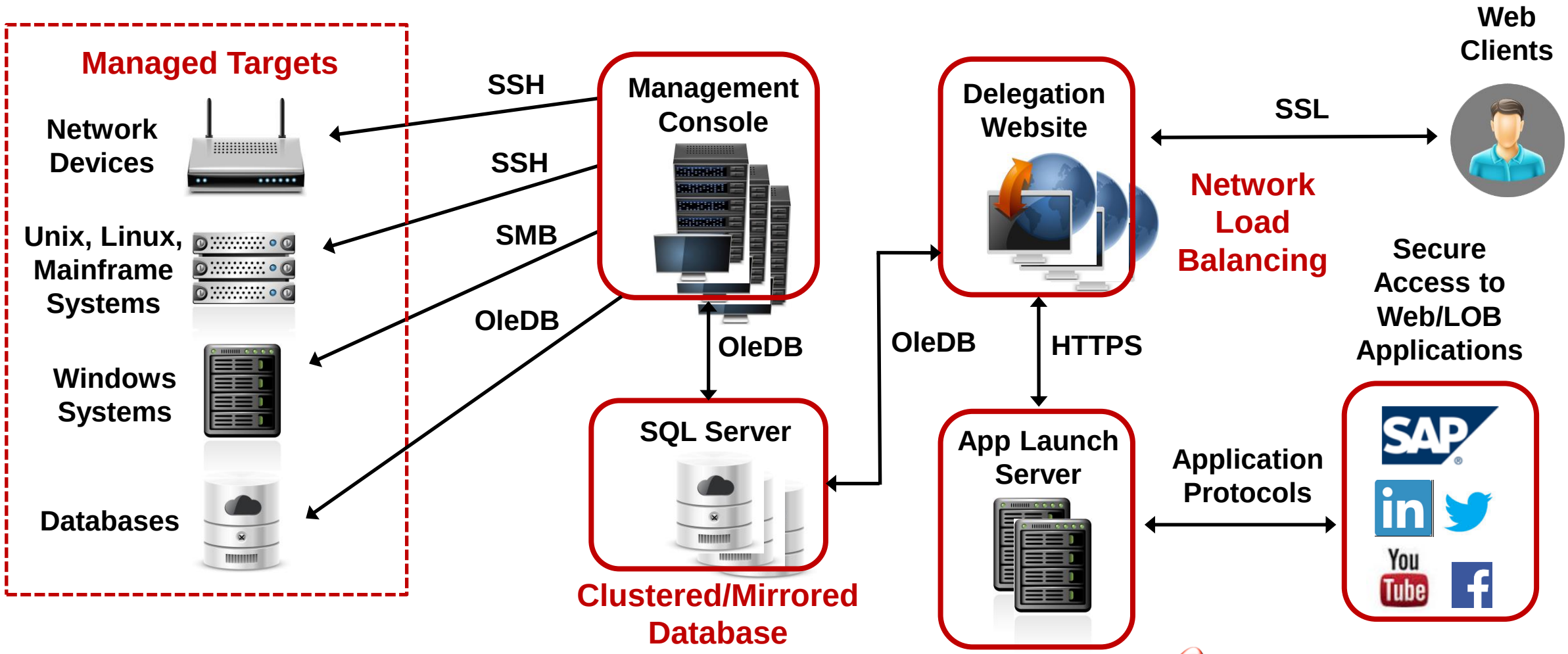
Почему привилегированные записи цель всех атак?

Защита периметра не спасает привилегированные «учётки»

Как минимизировать последствия компрометации?

Lieberman Software ERPM – автоматизированное управление привилегиями

Lieberman Software ERPM – автоматизированное управление привилегиями



Платформы поддерживаемые ERPM

Computer Hardware

- Windows
- UNIX
- Linux
- Dell DRAC
- HP iLO …

Databases

- SQL Server
- Oracle
- MySQL
- DB2
- Sybase …

Applications

- Microsoft System Center
- SharePoint
- McAfee ePO
- IBM BigFix
- SAP …

Network Appliances

- CheckPoint
- Cisco IOS
- EMC
- Foundry
- Juniper
- NetApp …

Mainframes

- AS/400
- OS/390
- z/OS …

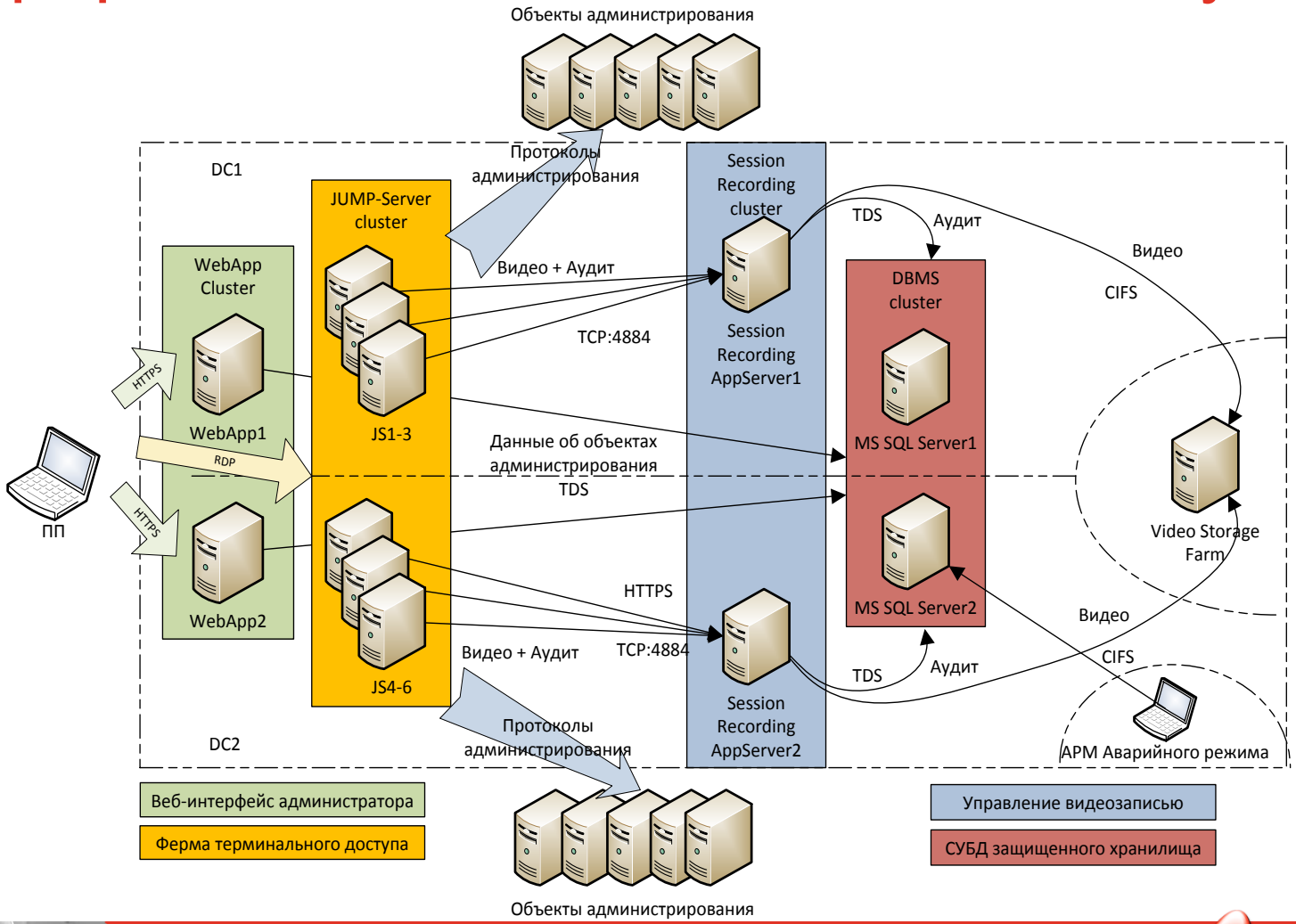
Middleware

- Proxy Accounts
- Gateway Accounts
- WebSphere
- WebLogic …

VM Environments

- VMware
- IBM System Z
- Microsoft Hyper-V …

Решение на базе ERPM: Защищенная среда администрирования с видео и текстовым аудитом



Про компанию Lieberman Software

- Основана в 1978 – с 1994 является ISV
- Пионер и иноватор в Privilege Management
- 1200+ клиентов во всех вертикалях
- Анализируется компаниями: Gartner, Forrester, 451 Group, Kuppinger-Cole

SC MAGAZINE

TECHWORLD AWARDS WINNER 2013

CRN Channel CHIEFS 2014

Security Products' GOVIES 2013 Government Security Awards

LeadershipCompass KuppingerCole
Market Leader
Privilege Management
January 2014

LeadershipCompass KuppingerCole
Innovation Leader
Privilege Management
January 2014

LIEBERMANSOFTWARE™

1200+ Корпоративных клиентов

Federal Government

MIT Lincoln Laboratory
U.S. Department of Homeland Security
U.S. Army
Federal Aviation Administration
U.S. Department of Transportation Federal Highway Administration
U.S. Department of Justice
USDA
VA

Finance

Bessemer Trust
cme Chicago Mercantile Exchange
Commerzbank
euroclear
GM Financial
Heartland Financial USA, Inc.
VISA
Wells Fargo

Healthcare

Centene Corporation
Innovative Hospice Care VITAS
HealthSouth
Temple University Health System
Vanderbilt University Medical Center
Shands HealthCare
South Georgia Medical Center
Mayo Clinic

Insurance

Arch Reinsurance Ltd.
Blue Cross Blue Shield
Delta Dental
Mutual of Omaha
GEICO
Assurity Life Insurance Company
Prudential
The Hartford

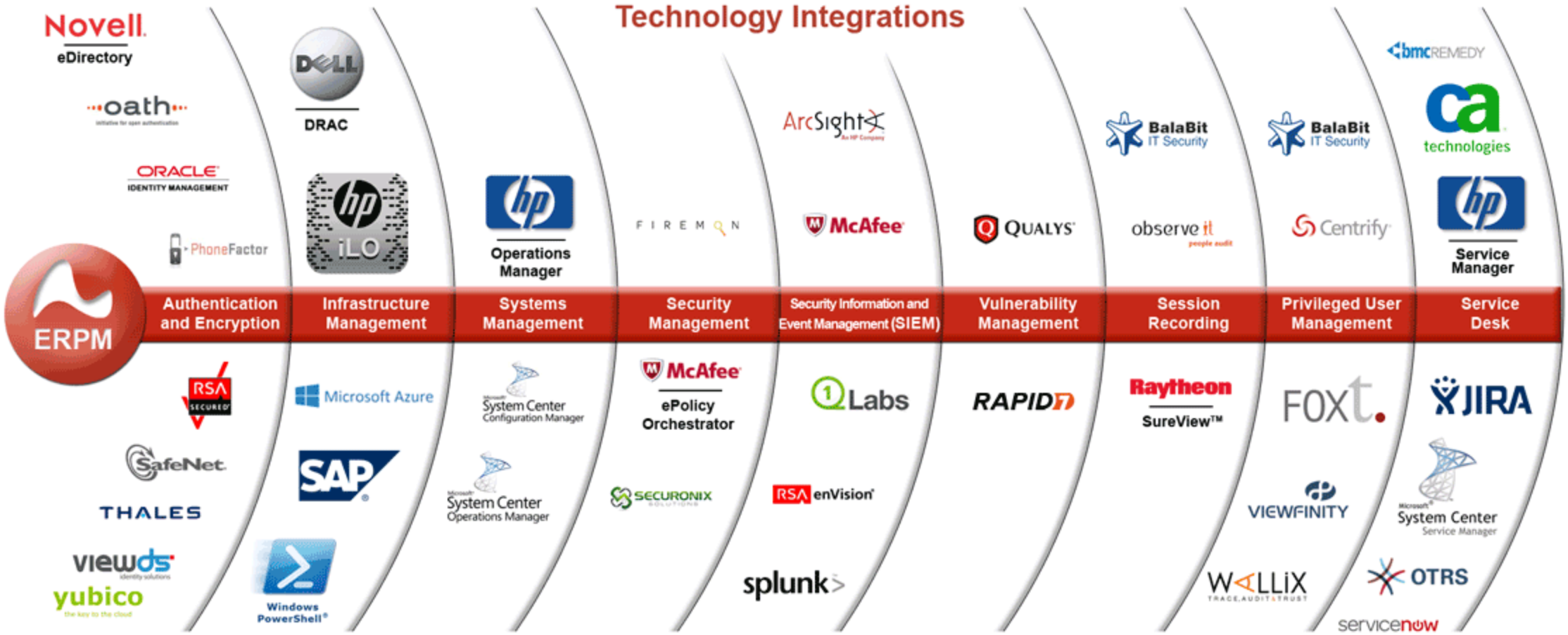
Manufacturing

Alcoa
Carpenter
Emerson Process Management
Cargill
Mattel
General Atomics
Micronas
Trane

Technology

Applied Materials
at&t
CSC
Dell Services
RSA
Thales
Microsoft
symantec.

Высокий уровень интеграции



Вопросы?

Спасибо!

Спасибо!

For more information:

Contact: