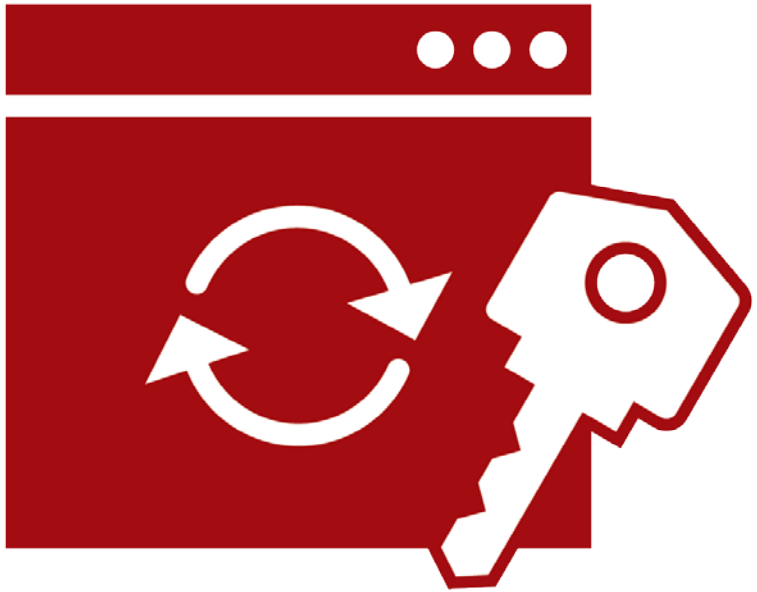
webcontrol

Lieberman RED Identity Management. Упреждающая защита

Николай Валаев

Краткое содержание

- Ландшафт угроз безопасности – новые реалии
- Привилегированная УЗ – первичная цель атаки
- Стратегия защиты – меняем пароли до, не после
- О программном обеспечении Lieberman



Защиты периметра недостаточно

Модель угроз меняется –

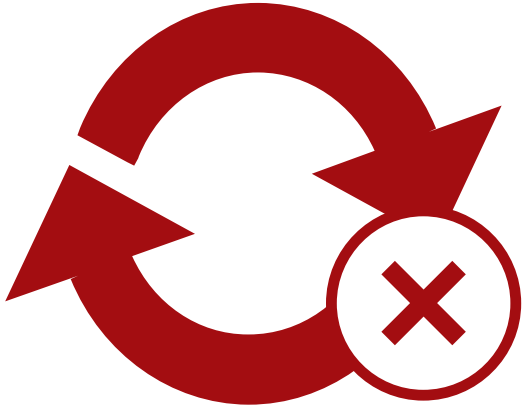
должны меняться

средства защиты

Почему недостаточно- болезненная правда

Решения по обнаружению и реагированию имеют проблемы

- Антивирусное программное обеспечение, брандмауэры, ПО защиты конечных точек работают... не всегда
- Что происходит автоматически при обнаружении вторжений?
- Что происходит, если вторжение не обнаружено?
- Как Вы устраняете последствия вторжения?



Взломы: статистика и цифры

Что говорят исследования

"The mean time to identify a data breach is **201 days.**"

2016 Cost of Data Breach Study - Ponemon Institute LLC

"**63%** of confirmed data breaches involved leveraging weak, default or stolen passwords."

2016 Data Breach Investigations Report - Verizon

"**70%** of breaches involving insider misuse took months or years to discover."

2016 Data Breach Investigations Report - Verizon

"...proactively managing credentials for privileged access actually reduces an organization's risk of a data breach by **75 to 80%**

How Managing Privileged Access Reduces the Risk of a Data Breach - Aberdeen Group

Анатомия атаки

Методология – мат в 5 ходов

1 Внешняя разведка
Определить слабое звено

- Начинается с одной уязвимости

2 Первоначальная компрометация
Исходное вторжение через целевой фишинг, социальную инженерию и т. Д.

- Зачастую хакеры «ловят» нужные УЗ по несколько месяцев

3 Плацдарм захвачен
Получены привилегированные УЗ (например, администратор домена)

PIM останавливает их На этапе 3

4 Внутренняя разведка
Расширение присутствия на доступные IP

- Захват распространяется быстро за счет слабо защищенных привилегированных УЗ

5 Миссия выполнена
Вывод данных

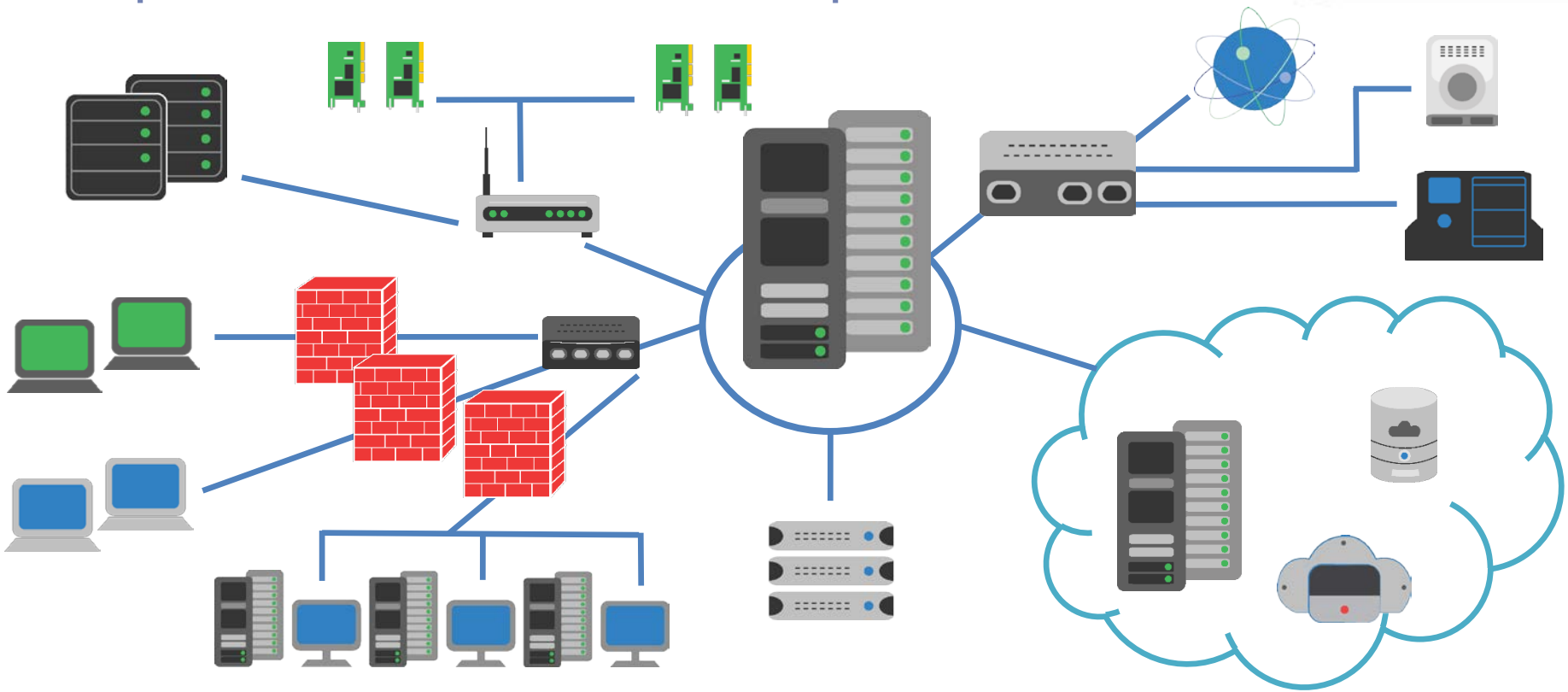
- Вы - в заголовках новостей ... по нерадостной причине

Почему привилегированные учетные записи – первичная цель атакующих

Доминанта:

Не дать украсть «ключи от королевства» -
УЗ Администратора Домена, root, su, etc….

Проблема УЗ - их много и разных

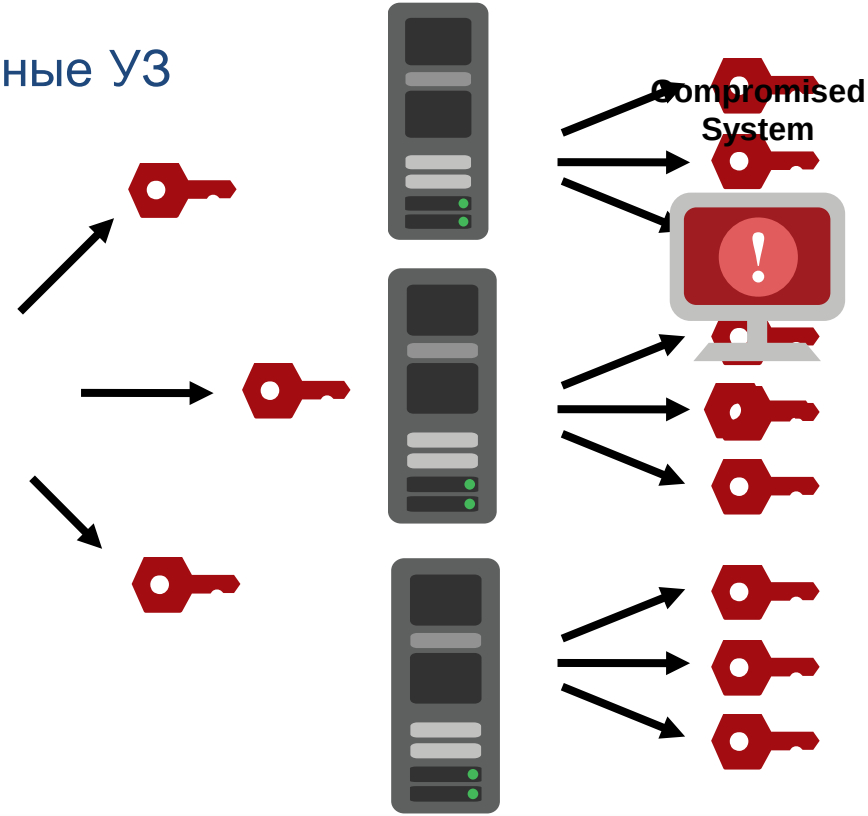


Как расширяется атака

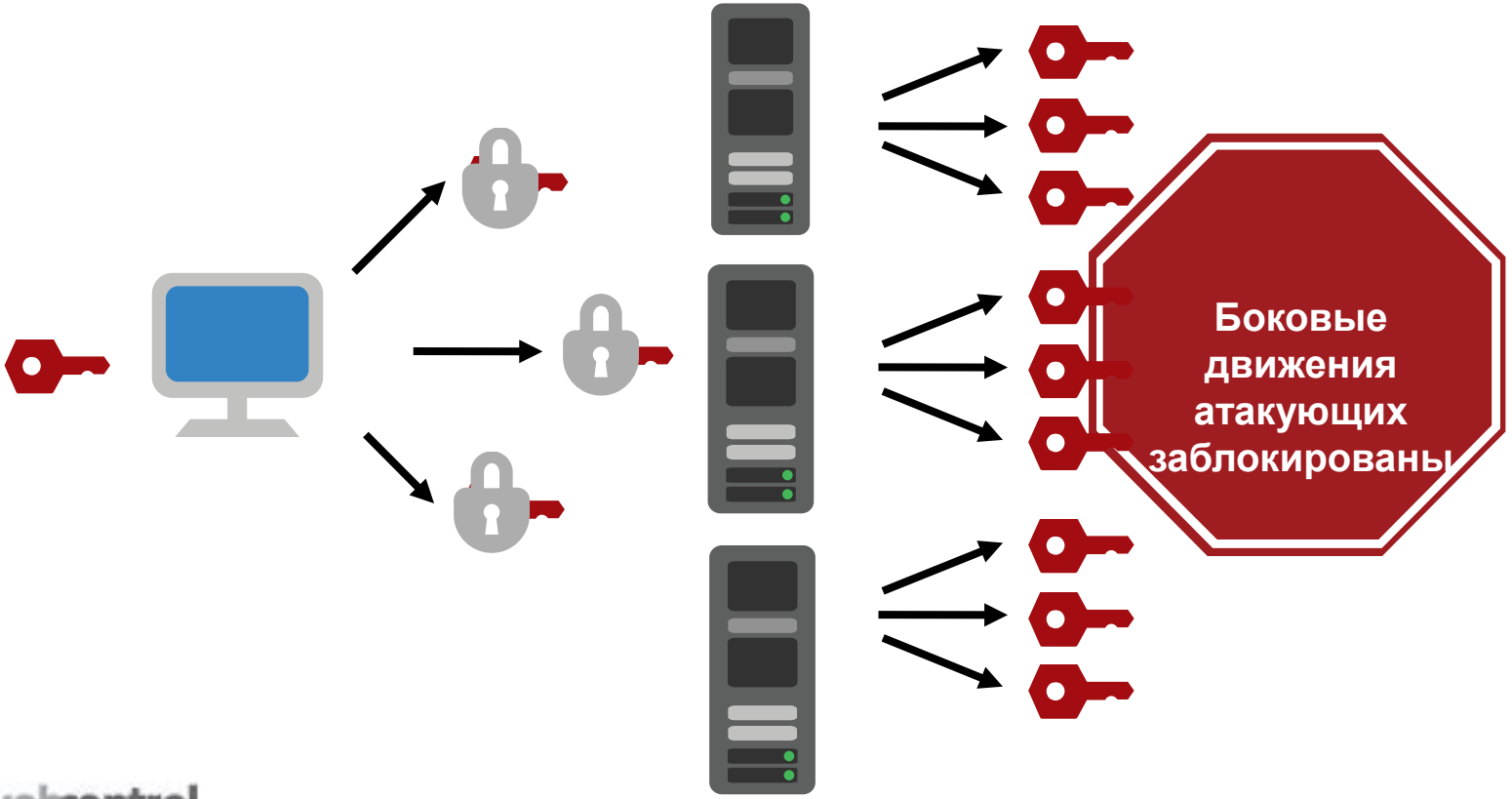
Через неуправляемые привилегированные УЗ

Слабый пароль привилегированной учетной записи легко добывается.
Key Logging……..
Очень часто УЗ имеет доступ ко многим, многим, многим, ресурсам

Атакующие прыгают с системы на систему, используя ненадежные привилегированные учетные записи



Меняйте пароли заранее



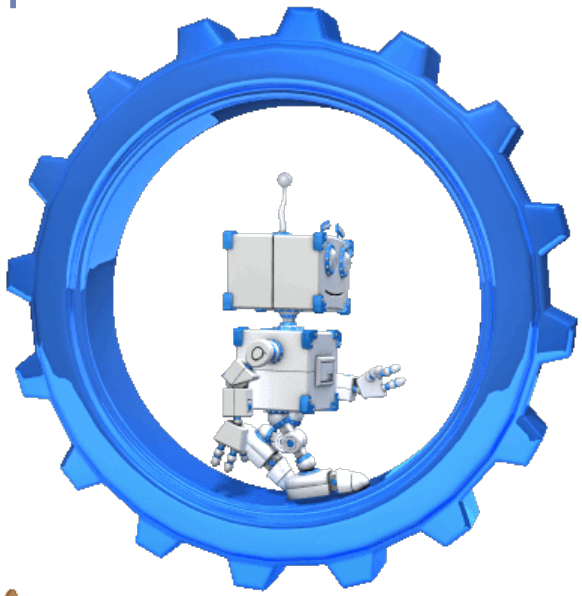
Непрерывная смена паролей делает сниффинг бесполезным

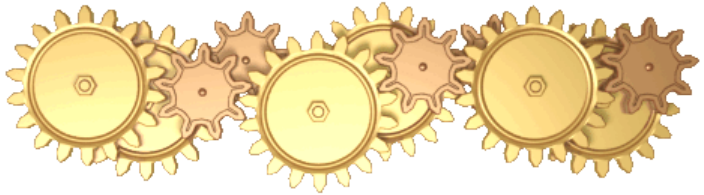
Хакерам трудно попасть в движущуюся цель

- **Контролируемые сроки использования пароля ограничивают значение «скомпрометированных учетных данных»**
- **Масштабирование и автоматизация могут изменять учетные данные так же часто, как каждый день или даже каждый час**

Необходимость автоматизации и скорости

- **Ваши оппоненты автоматизированы. Вы должны быть автоматизированы.**
- **Пароли необходимо изменять в часы, а не в дни или в недели.**





Комплексное решение: Lieberman RED Identity Management

LIEBERMAN RED

LIEBERMANSOFTWARE

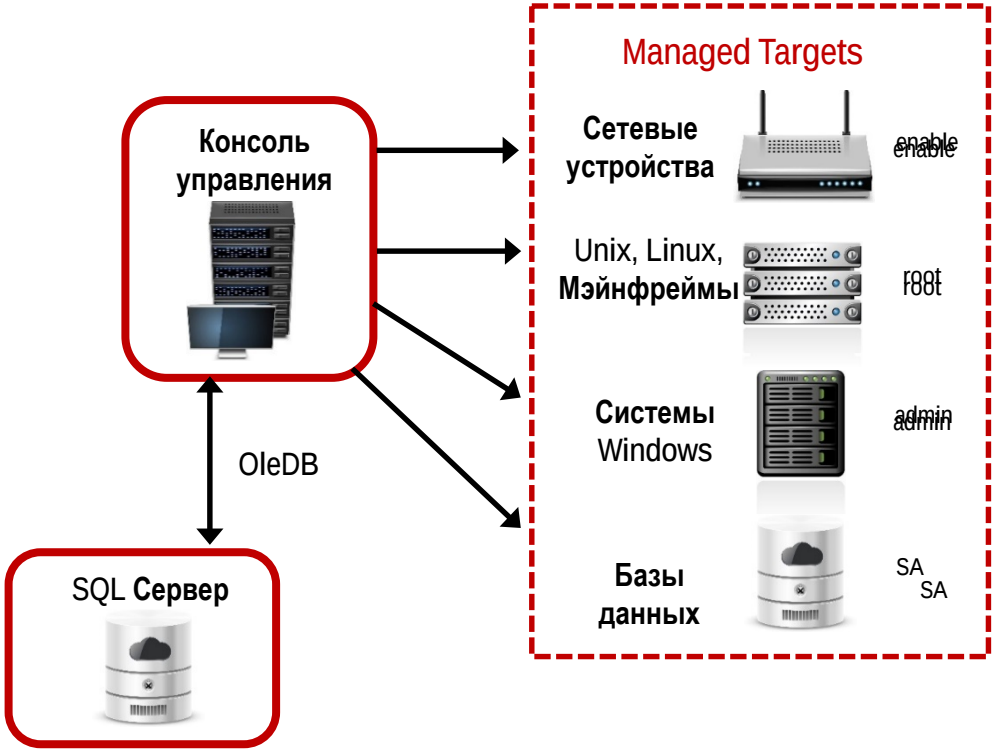
Комплексная платформа

webcontrol

Автопоиск систем, аккаунтов и их использования

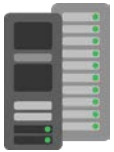
- Сканирование систем
- Перехват соблюдения парольной политики привилегированных УЗ

Asset	Account	Password
Router	enable	[illegible]
Linux	root	[illegible]
Windows	Admin	[illegible]
Database	SA	[illegible]



Поддерживаемые платформы

Практически каждый ИТ-активов, на месте, и в облаке



Compute r Hardware

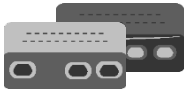
- Windows
- UNIX
- Linux
- Dell DRAC
- HP iLO …

Databases

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

Application s

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

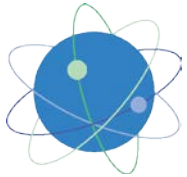


Network Appliances

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

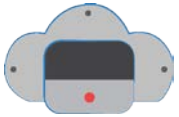
Mainframe s

- AS/400
- OS/390
- z/OS …



Middlewar e

- Proxy Accounts
- Gateway Accounts
- WebSphere
- WebLogic …



VM Environments

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

Технология автообнаружения

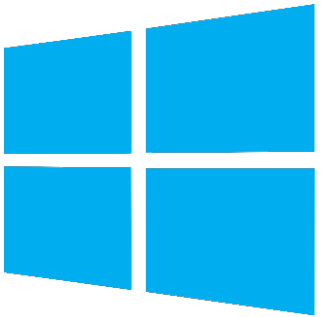
Широкий спектр методов обнаружения систем и учетных записей

- **Настройте решение один раз с минимальным ручным трудом**
- **Методы автоматического обнаружения извлекают из доменов, AD / LDAP, IP-адресов, CMDB и т. Д.**
- **Сетевой уровень сканирует устройства**

Windows

Отличное обнаружение и использование УЗ

- **Поддерживает встроенное обнаружение учетных записей на всех видах** Windows
- **Использует API, специфичные для целевой подсистемы (не WMI)**
- **Автоматическое обнаружение и использование учетных записей документов в службах, задачах, COM / DCOM, IIS, и многое другое**



Linux / UNIX

- Сканирование сети, определение систем Linux и управление ими
- Автоматически находить учетные записи, пары ключей SSH, политики sudo и многое другое
- Постоянная смена паролей учетных данных
- Используйте отчеты о политике SUDO, чтобы узнать, какие политики применяются на любом хосте

Clouds

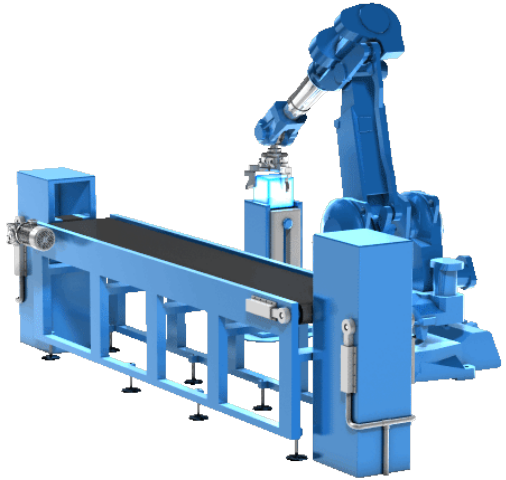
Защищать облако внутри и снаружи

- **Находить и управлять привилегированными УЗ облачной платформы**
- **Обнаруживать и защищать УЗ и системы, управляющие базовыми облачными платформами**

SSH

Преодоление уязвимостей SSH

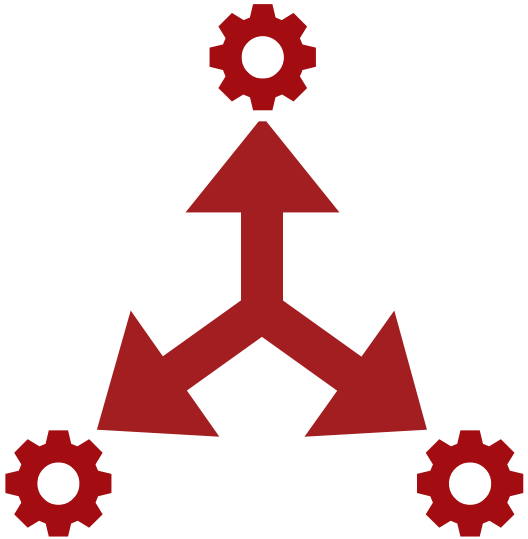
- **Автоматическое обнаружение, корреляция и ротация ключей SSH**
- **Используйте SSH-ключи для подключения и управления учетными данными на целевых системах**
- **Автоматически подключайте пользователя к целевой системе с определенным приложением, ограничивая доступ к определенным командам и аутентификации**
- **Устраните необходимость прямой связи с системами** Linux / UNIX **с прокси-соединениями SSH**



Службы и приложения

Динамическое использование и распространение УЗ

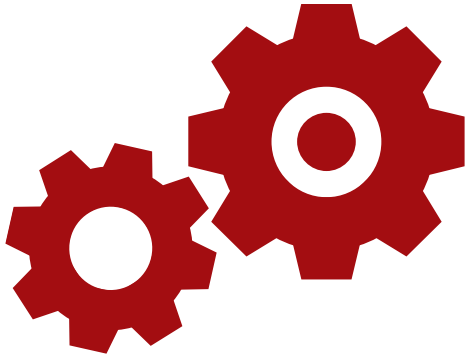
- **Автоматическое обнаружение зависимостей учетной записи службы**
- **Распространять пароли во всех ссылочных местоположениях в каждой подсистеме - так что ничего не сломается**
- **Остановить учетные записи службы в правильном порядке, изменить корневую службу, а затем перезапустить все службы**
- **Изменение паролей в приложениях, сценариях, файлах и местах, где связаны учетные записи**



Интегрированная аутентификация

Безопасный, оптимизированный пользовательский доступ

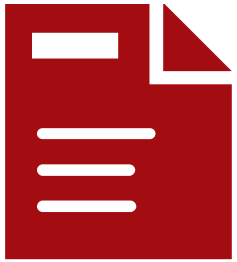
- **Поддержка нескольких форм аутентификации пользователей:**
  - Облачные платформы: Azure AD и SalesForce.com
  - Доверенные / недоверенные домены Windows через пользователей и группы
  - Каталоги LDAP
  - Сертификаты (смарт-карты, CAC / PIV и т. Д.)
  - База данных внутренних счетов
- **Интеграция с поставщиками** MFA: RSA SecurID, YubiKey, OATH, PhoneFactor, SafeNet, RADIUS **и т. Д.**



Аудит, журналирование, отчетность

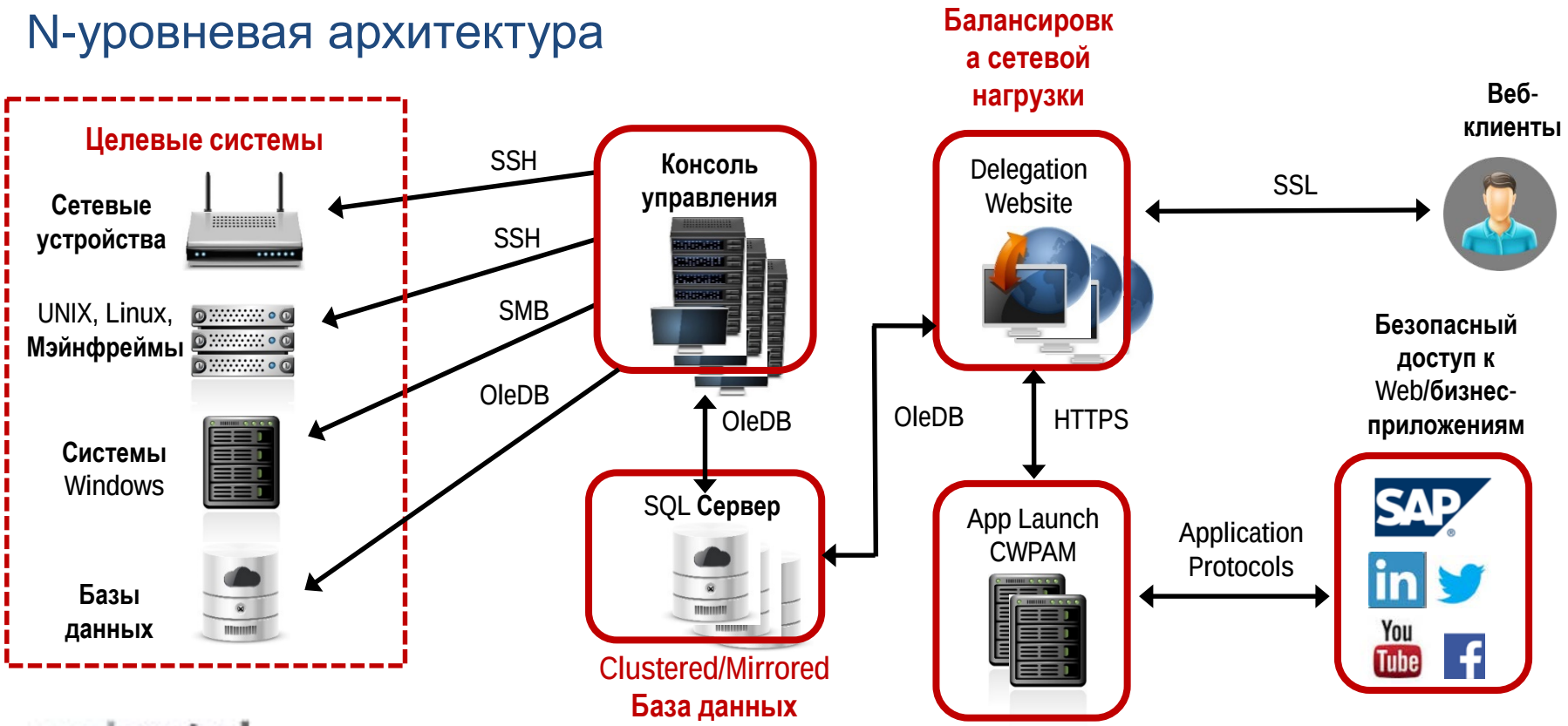
Обеспечение соблюдения нормативных требований

- **Зарегистрировать пароль, системную и пользовательскую активность**
- **Предоставление комплексных отчетов о проверке и соблюдении**
- **Отображать панели мониторинга в реальном времени для быстрого просмотра активности продукта, пользователя, системы или управляемого учетной записи**
- **Настраивать оповещения для отправки электронной почты, запускать программы, общаться с другими приложениями, выводить данные событий в** syslog / other framework
- **Интеграция с системами SIEM, платформами IGA, приложениями для подачи заявок на проблемы и т. Д. Для аудита закрытой проверки привилегированной деятельности**



Архитектура

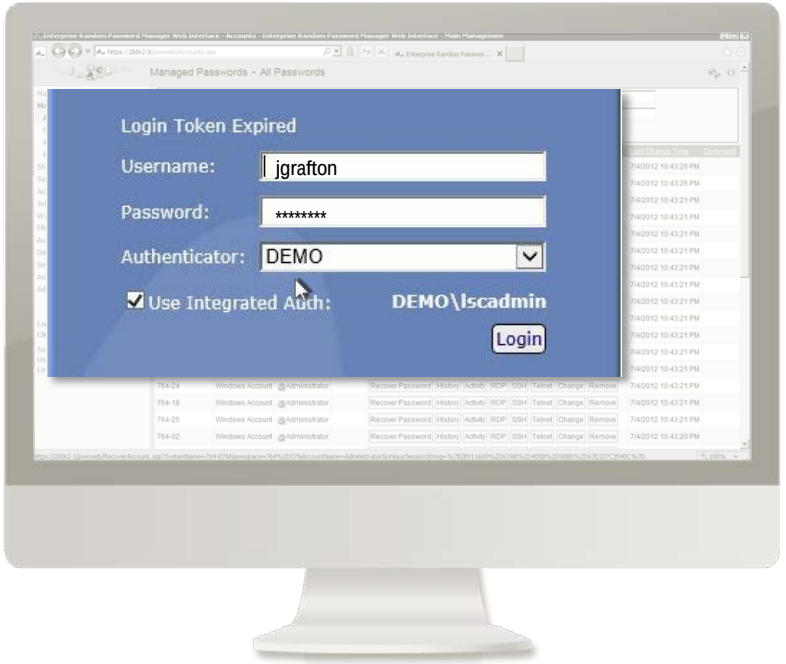
N-уровневая архитектура



Хорошо расширяемое решение

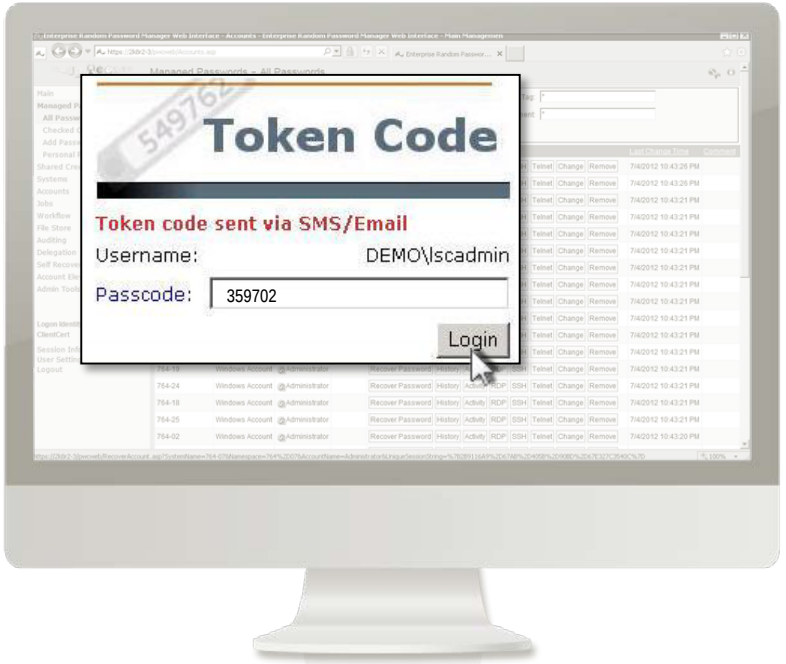
Предоставление доступа пользователю

1. Пользователь вводит ID / пароль корпоративной учетной записи



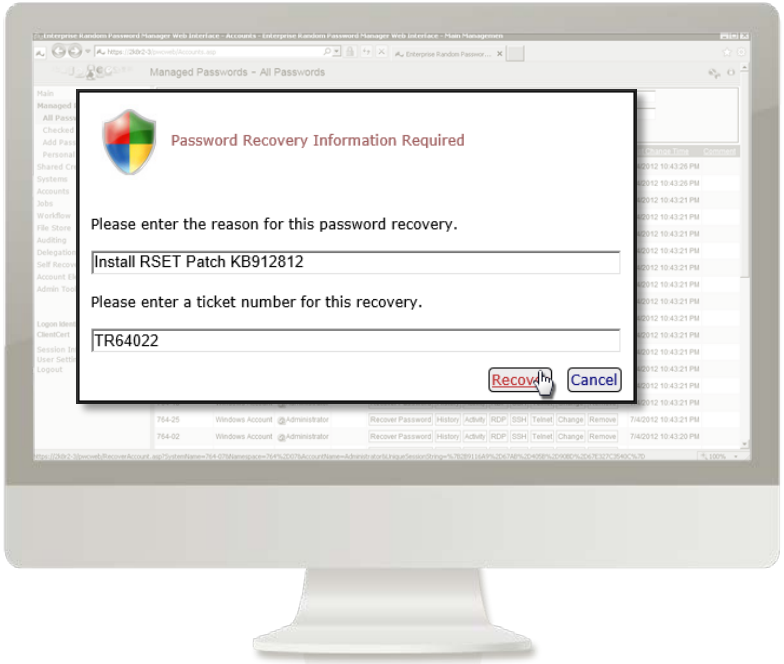
Предоставление доступа пользователю

1. Пользователь вводит ID / пароль корпоративной учетной записи
2. Подтверждает мультифакторной аутентификацией
(RSA Token)



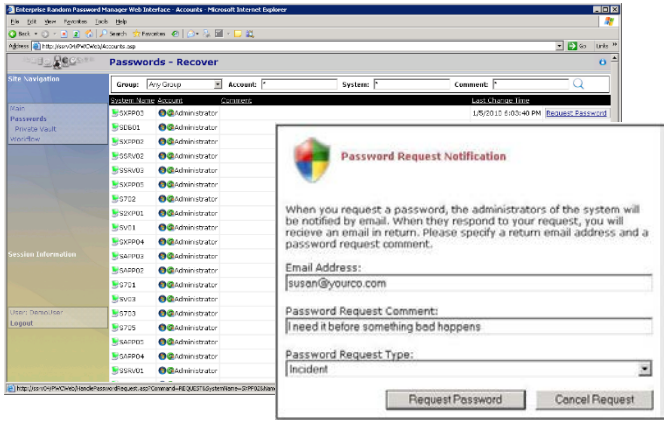
Предоставление доступа пользователю

1. Пользователь вводит ID / пароль корпоративной учетной записи
2. Подтверждает мультифакторной аутентификацией (RSA Token)
3. Проверяет заявку и документирует причину для доступа



Предоставление доступа пользователю

1. Пользователь вводит ID / пароль корпоративной учетной записи
2. Подтверждает мультифакторной аутентификацией (RSA Token)
3. Проверяет заявку и документирует причину для доступа
4. Запрашивает доступ в соответствии с рабочими процессами



Предоставление доступа пользователю

1. Пользователь вводит ID / пароль корпоративной учетной записи
2. Подтверждает мультифакторной аутентификацией (RSA Token)
3. Проверяет заявку и документирует причину для доступа
4. Запрашивает доступ в соответствии с рабочими процессами
5. Получает доступ к ресурсу.

О программном обеспечении Либерман?

- **Основана в** 1978 – 1994 **как независимый поставщик ПО** (ISV)
- **Пионеры и новаторыуправления привилегиями**
- **Отслеживает** Gartner, Forrester, 451 Group, Kuppinger-Cole
- **Нет открытого кода**.
- **Управляется владельцем**.

1400+ Enterprise Customers Worldwide

Finance & Insurance

Entertainment

Consumer & Retail

Technology & Manufacturing

Government

Energy & Utilities

Healthcare

And many more!

Вопросы?

Спасибо!

LIEBERMAN RED

LIEBERMAN SOFTWARE