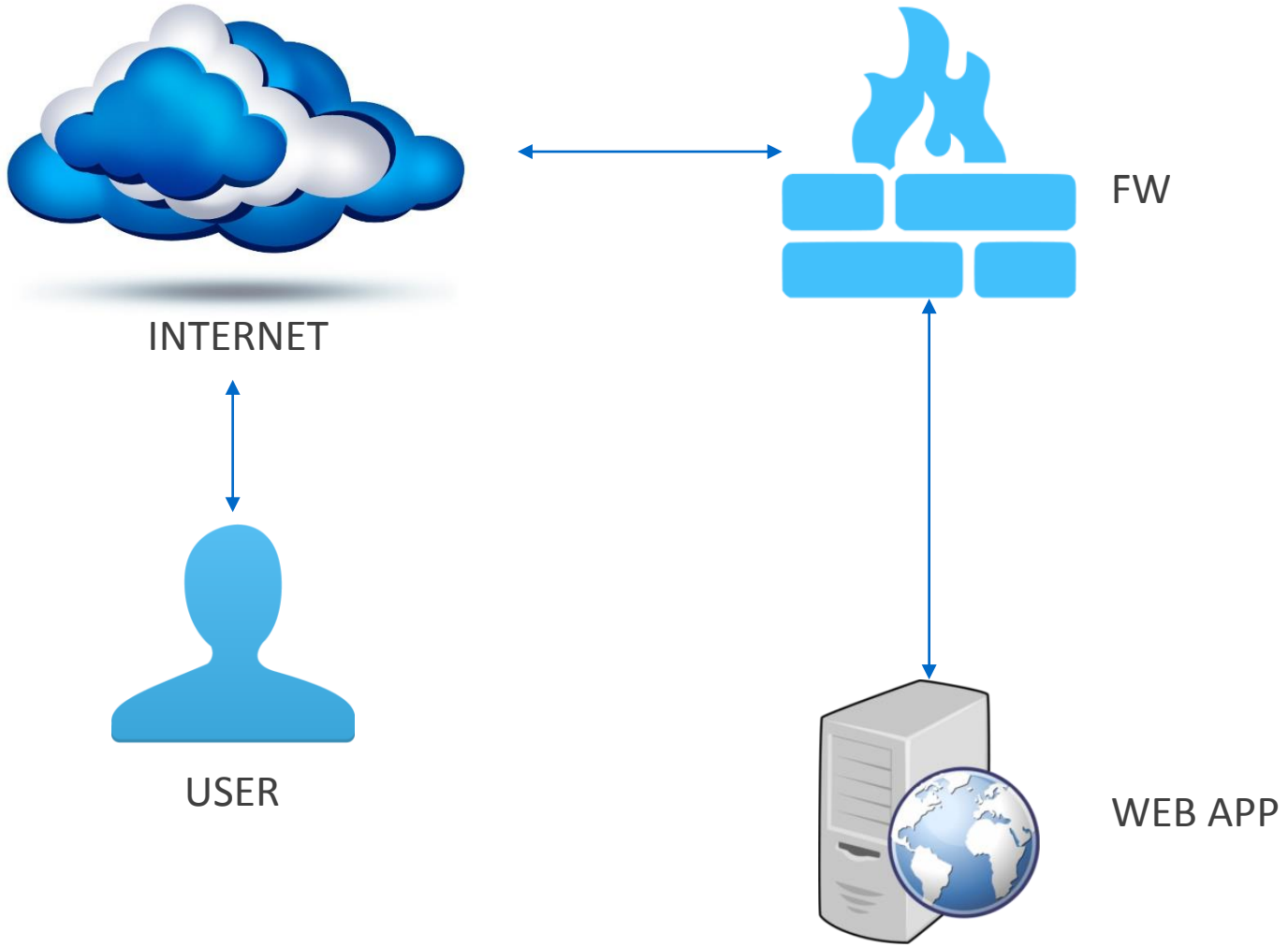
Rapid7 | Barracuda Networks

Не дай себя взломать

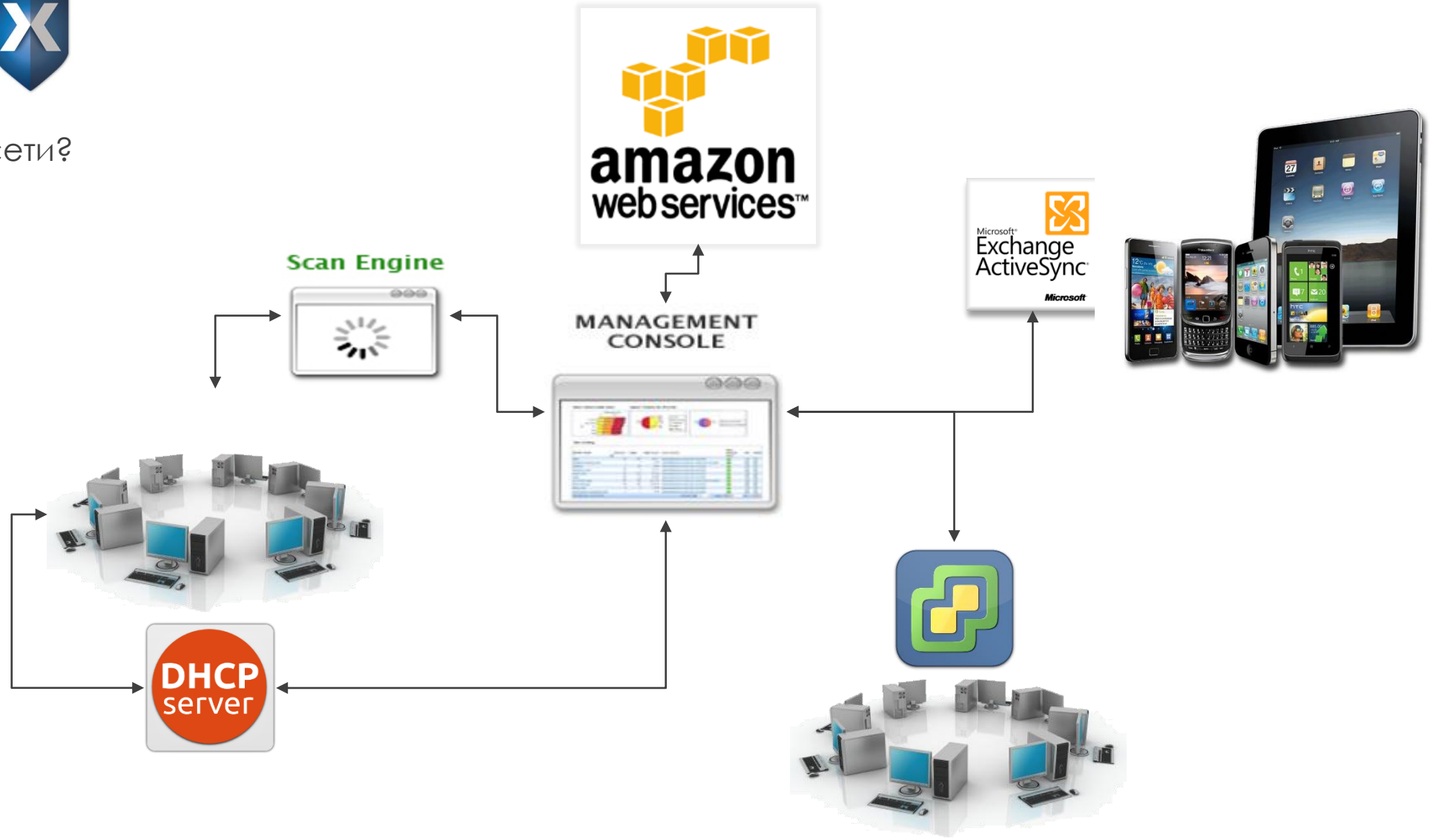
Softprom by ERC
Роман Розумей | Инженер ИБ


INTERNET
FW
USER
WEB APP

Уязвимы ли вы?

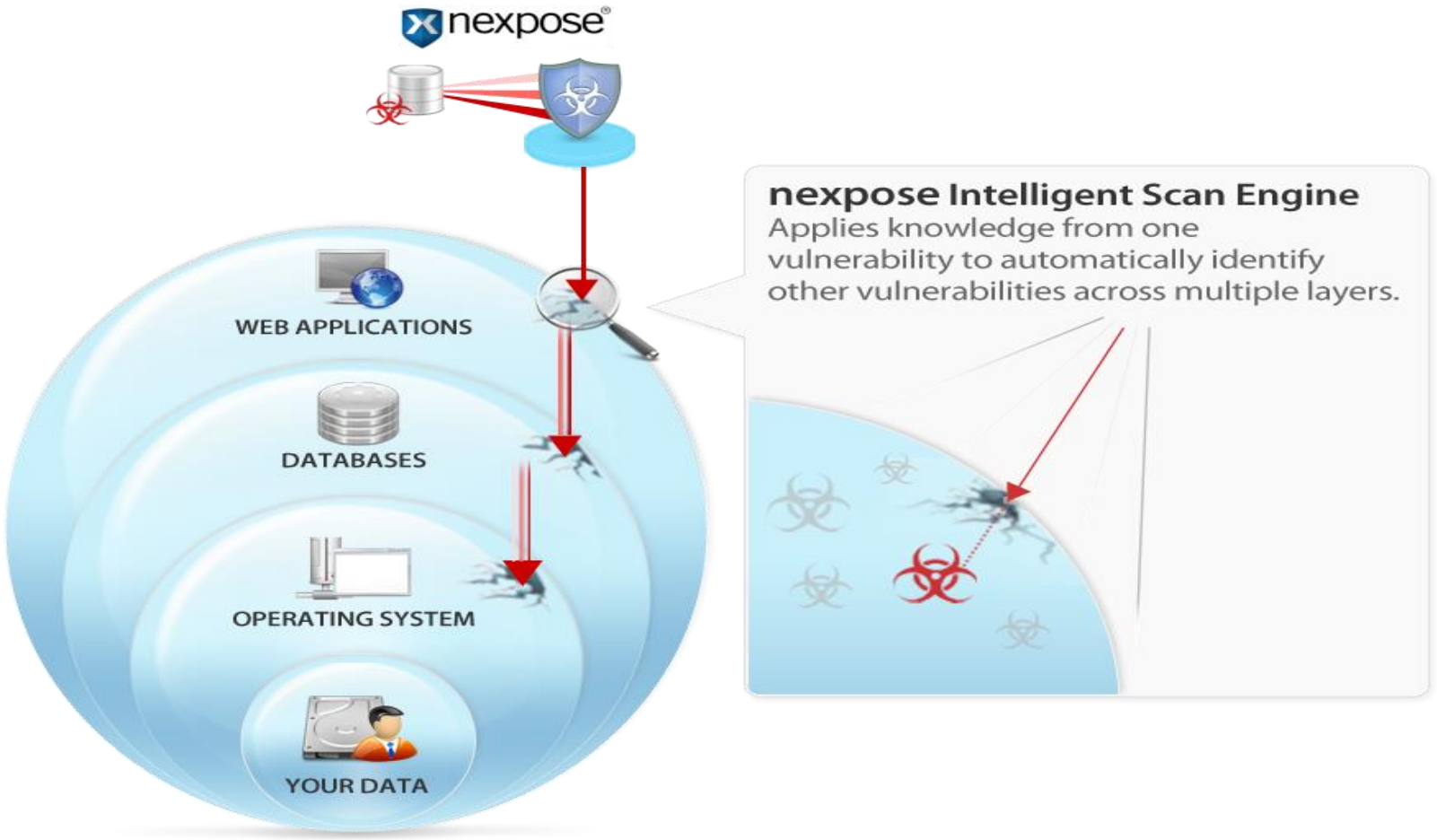
Nexpose

Что есть в вашей сети?



Nexpose

>180 000 + Проверок на наличие уязвимостей



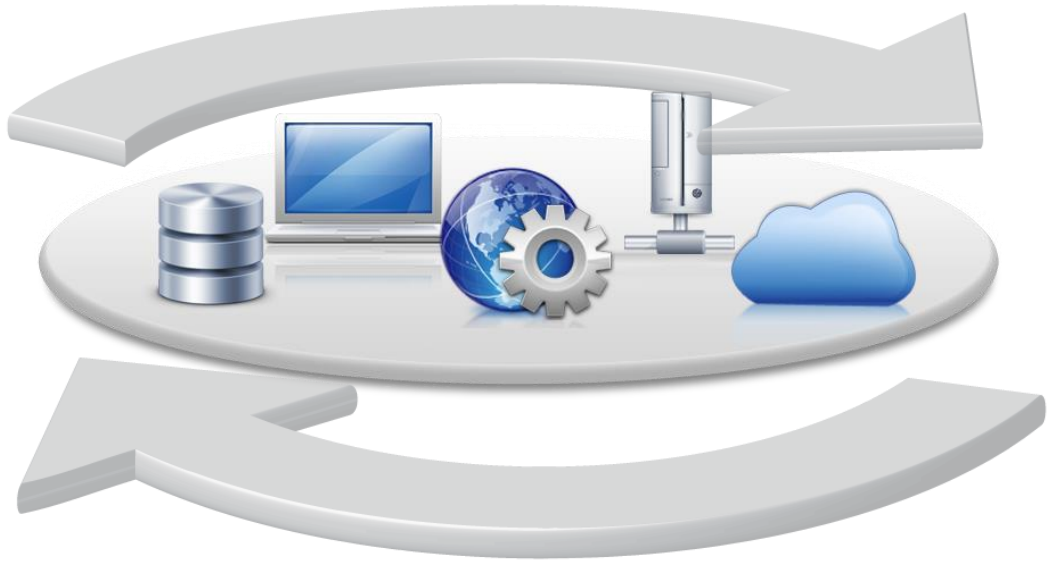
Уязвимостей слишком много?

Metasploit

Квалификация уязвимости

nexpose®

Управление уязвимостями и проверка конфигураций



metasploit®

Тестирование на проникновение и подтверждение угроз

Верификация уязвимости

Metasploit

Другие векторы проникновения

Возможность проводить фишинговые атаки посредством:

- Писем
- Сайтов
- Сьемных дисков
- Исполняемых файлов

С последующим установлением сессии с уязвимым хостом

Как бороться?

Nexpose

Планирование устранения уязвимостей

3.1. Remediation Plan for 10.3.60.136

3.1.1. For Microsoft Windows Server 2008 R2, Enterprise Edition SP1

These vulnerabilities can be resolved by performing the following 60 steps. The total estimated time to perform all of these steps is 29 hours 45 minutes.

Download and install Microsoft patch windows6.1-kb2778930-x64.cab (1608367 bytes)

Estimated time: 30 minutes

Microsoft Windows Server 2008 R2 SP1 OR < SP1 (x86_64), Microsoft Windows Server 2008 R2, Enterprise Edition SP1 OR < SP1 (x86_64), Microsoft Windows Server 2008 R2, Standard Edition SP1 OR < SP1 (x86_64), Microsoft Windows Server 2008 R2, Datacenter Edition SP1 OR < SP1 (x86_64), Microsoft Windows Server 2008 R2, Web Edition SP1 OR < SP1 (x86_64)

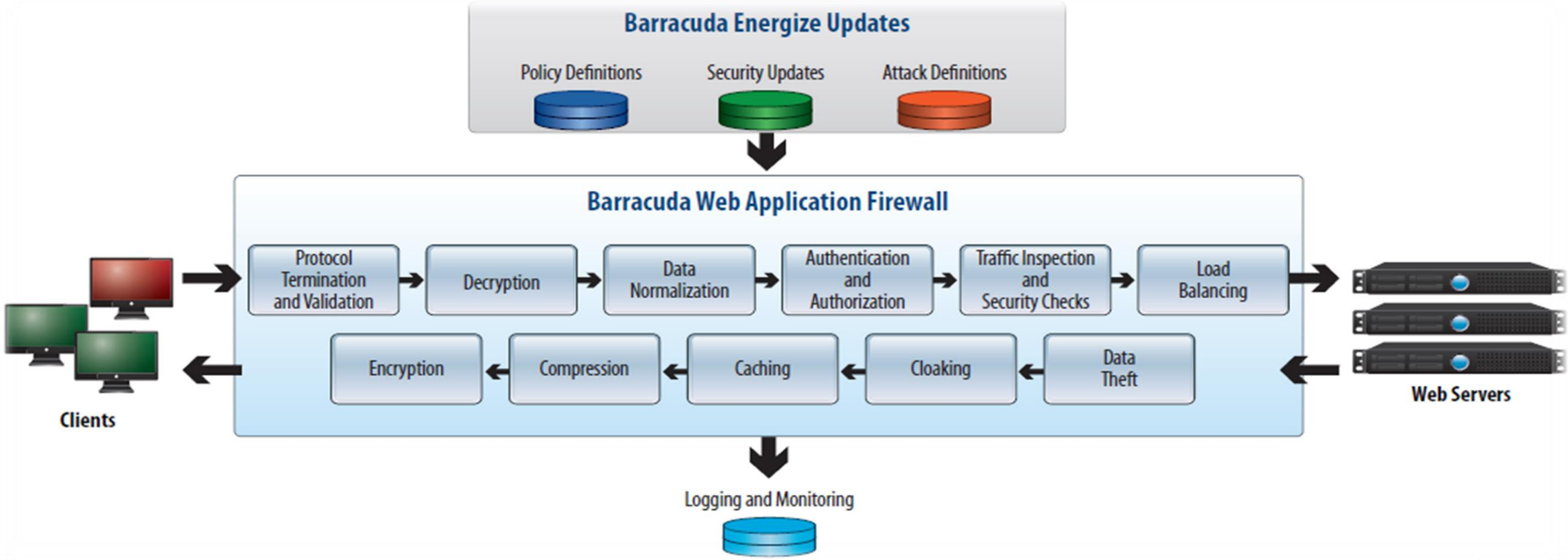
Download and apply the patch from: http://download.windowsupdate.com/msdownload/update/software/secu/2012/12/windows6.1-kb2778930-x64_f77ccab1701f0d386362e64b83a5783964cd7a52.cab

This will address the following 15 issues:

- MS11-012: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS11-012)
- MS11-034: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (WINDOWS-HOTFIX-MS11-034)
- MS11-041: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694) (WINDOWS-HOTFIX-MS11-041)
- MS11-054: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917) (WINDOWS-HOTFIX-MS11-

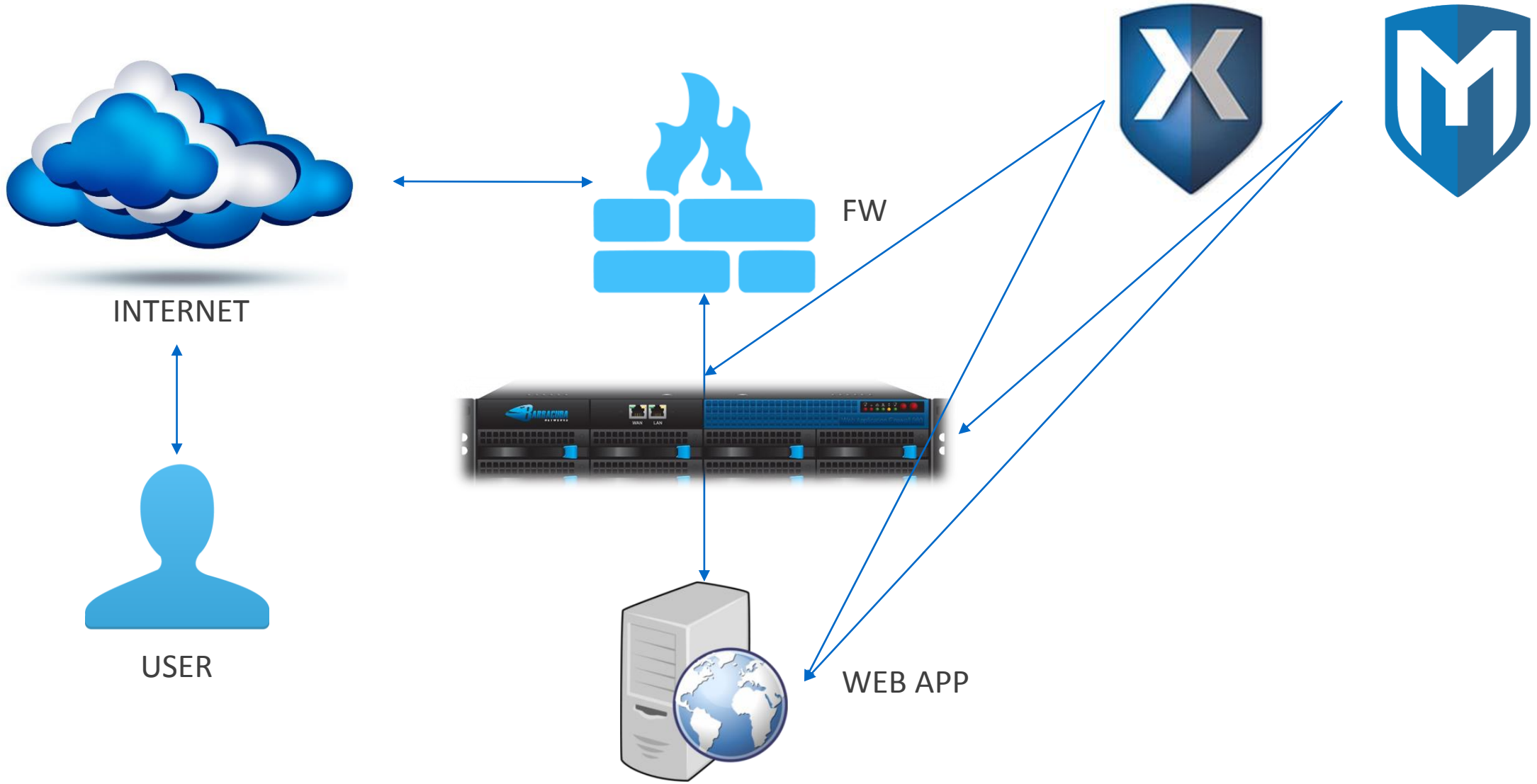
Barracuda WEB Application Firewall

Архитектура Barracuda Web Application Firewall



Безопасность веб-приложений

- Скрывает серверную информацию
- Защита против атак на 7-м уровне
- Защита данных от потери
- Интегрированная XML защита

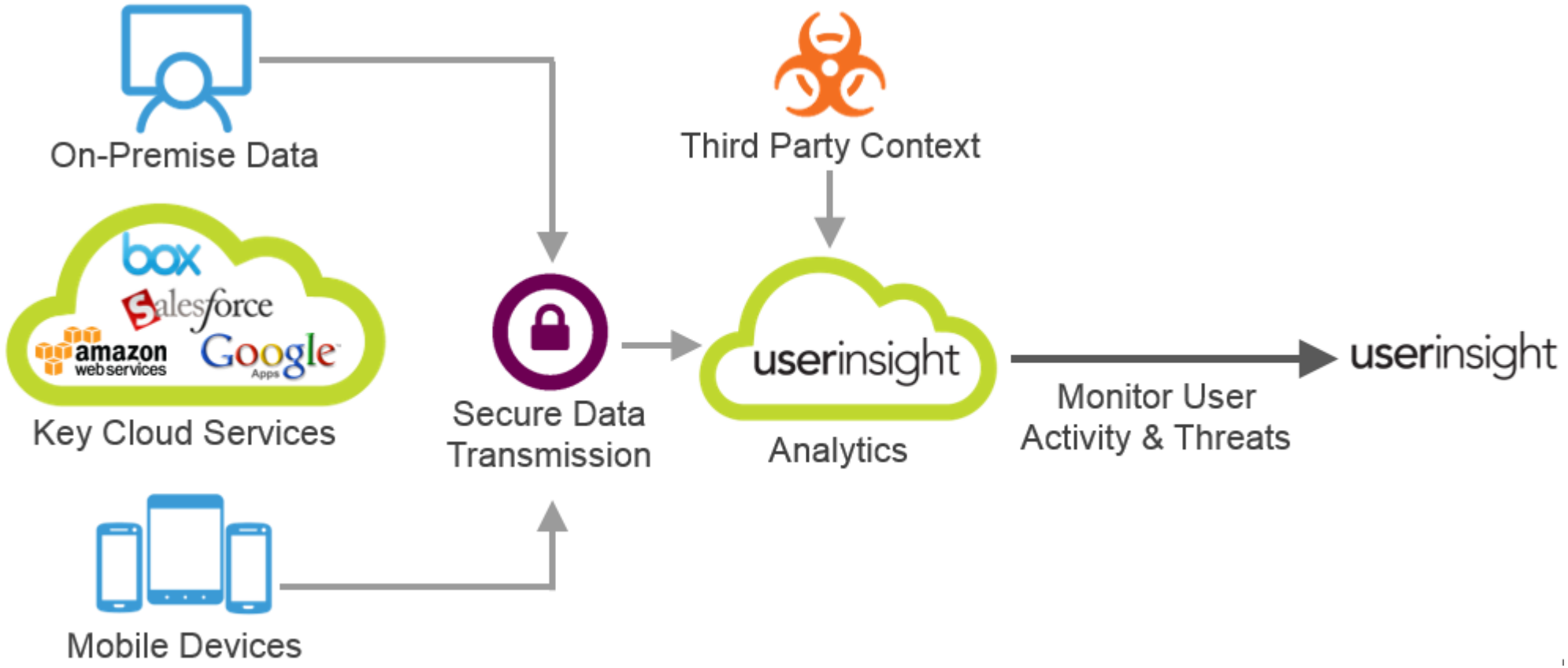

INTERNET
FW
USER
WEB APP

Демонстрация

Как вовремя узнать что вас взломали?

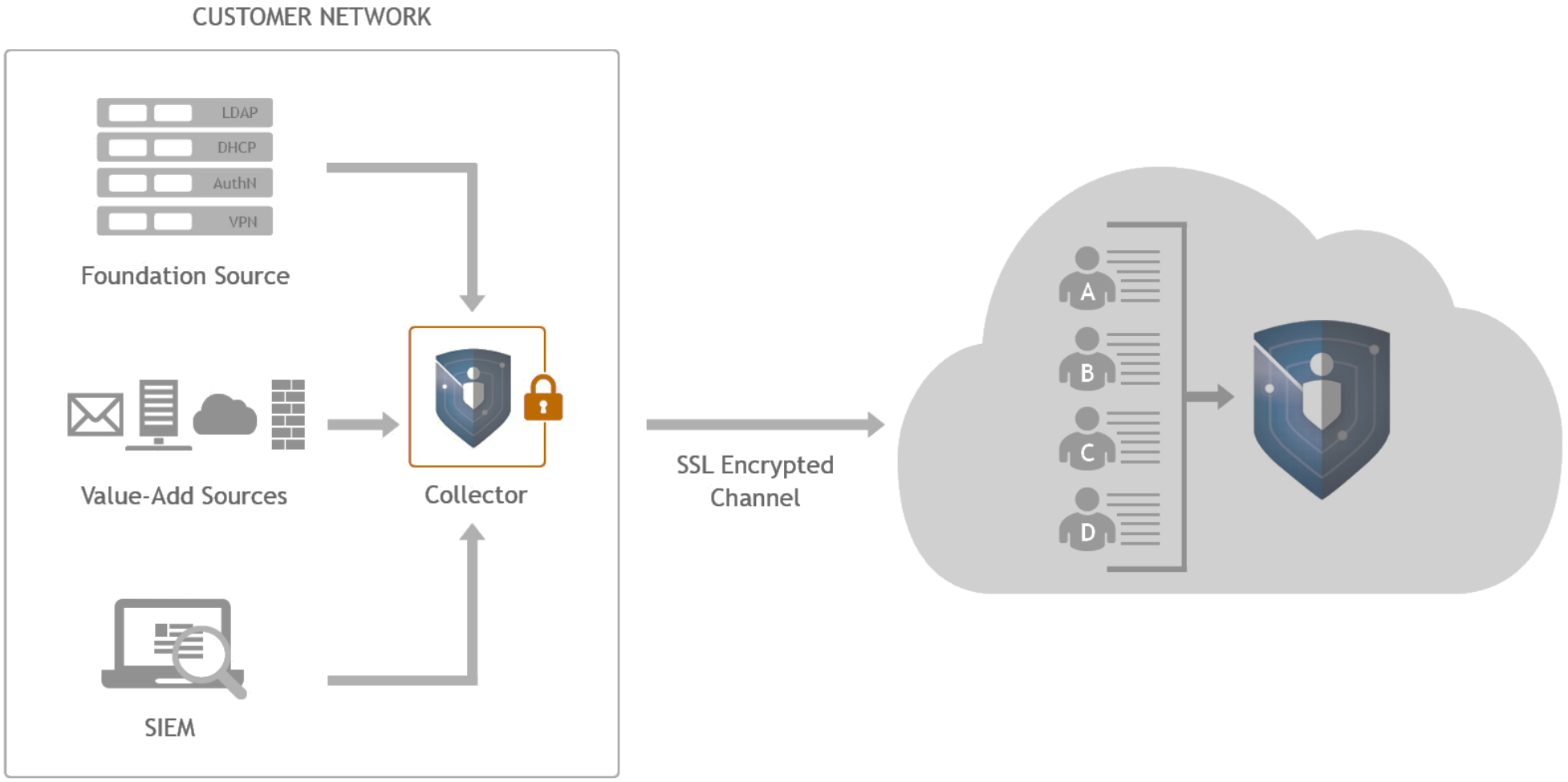
UserInsight

Глубокий анализ поведения пользователя и корреляция данных из различных источников для выявления подозрительной активности

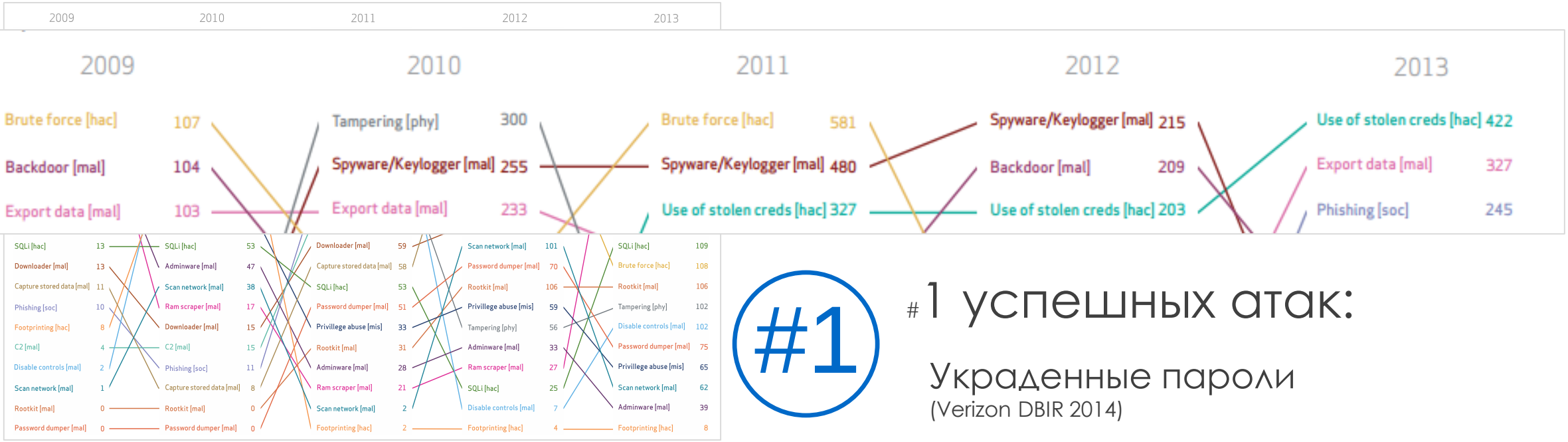


UserInsight

Как это работает



UserInsight



#1

#1 успешных атак:

Украденные пароли
(Verizon DBIR 2014)

"Пользователи остаются самым слабым звеном в защите"

Gartner 2013

UserInsight

Что в итоге

- Контролирует все активности пользователей
- Контролирует все активности администраторов
- Контролирует геоданные подключенных пользователей
- Обнаружение скомпрометированных аккаунтов
- Обнаружение попыток фишинга
- Обнаружение доступа злоумышленника к сети
- Выявляет неавторизованный доступ к критическим хостам
- Определяет попытки спрятать активность
- Автоматически сопоставляет данные о угрозах пользователях и хостах
- Выявляет нарушения политик и злоупотребление правами

Демонстрация

Связаться с нами

info@softprom.com