



Компания КОМПЛИТ



Комплексное решение по регламентации доступа к географически распределенным ИТ-ресурсам

www.complete.ru

Миронов Дмитрий
Старший Инженер

Универсальность, отказоустойчивость, безопасность, регламентация!

Задача построить:

Унифицированное решение на базе отказоустойчивого программно-аппаратного комплекса, позволяющее обеспечить защищенный безопасный удаленный доступ пользователей к географически распределенным внутренним ресурсам сети.



Система базируется на 2-х основных компонентах

- ✓ **CITRIX** NetScaler
- ✓ **CITRIX** XenApp



Основной компонент реализации унифицированного доступа

✓ **CITRIX NetScaler**



Основные функциональные особенности CITRIX NetScaler

- ✓ **Балансирует** запросы между географически разнесенными площадками;
- ✓ Осуществляет **сканирование** и анализ конечного устройства;
- ✓ Организует **гранулированный доступ** к различным сегментам сети посредством политик доступа;
 - ✓ Является **VPN-SSL решением** Enterprise уровня;
 - ✓ Позволяет реализовать функцию **аппаратного ICA-Proxy**.



Компонент терминального доступа к ИТ-ресурсам

✓ **CITRIX XenApp**



Терминальная система доступа компании CITRIX

- ✓ Де-факто **стандарт доставки терминальных приложений**;
- ✓ Интегрированная **потокковая** доставка и изоляция;
- ✓ Единое **централизованное хранилище** для всех клиентов приложений Windows;
 - ✓ Поддержка **до 500 пользователей** на сервер;
- ✓ Интегрированная **безопасность** (SSO, SSL VPN и WAN Оптимизация);
- ✓ Интегрированный **мониторинг производительности** (EdgeSight).



Компоненты, обеспечивающие дополнительный функционал системы



- ✓ Xceedium GateKeeper
- ✓ RSA Authentication Manager
 - ✓ ThinPrint .print ASE
 - ✓ CITRIX XenDesktop
 - ✓ CITRIX Branch Repeater
 - ✓ Observe IT



observe **it**
People audit

Компонент дополнительной меры безопасности при доступе к ресурсам

✓ **RSA Secure ID Authentication Manager**



Способы аутентификации – относительная стойкость.

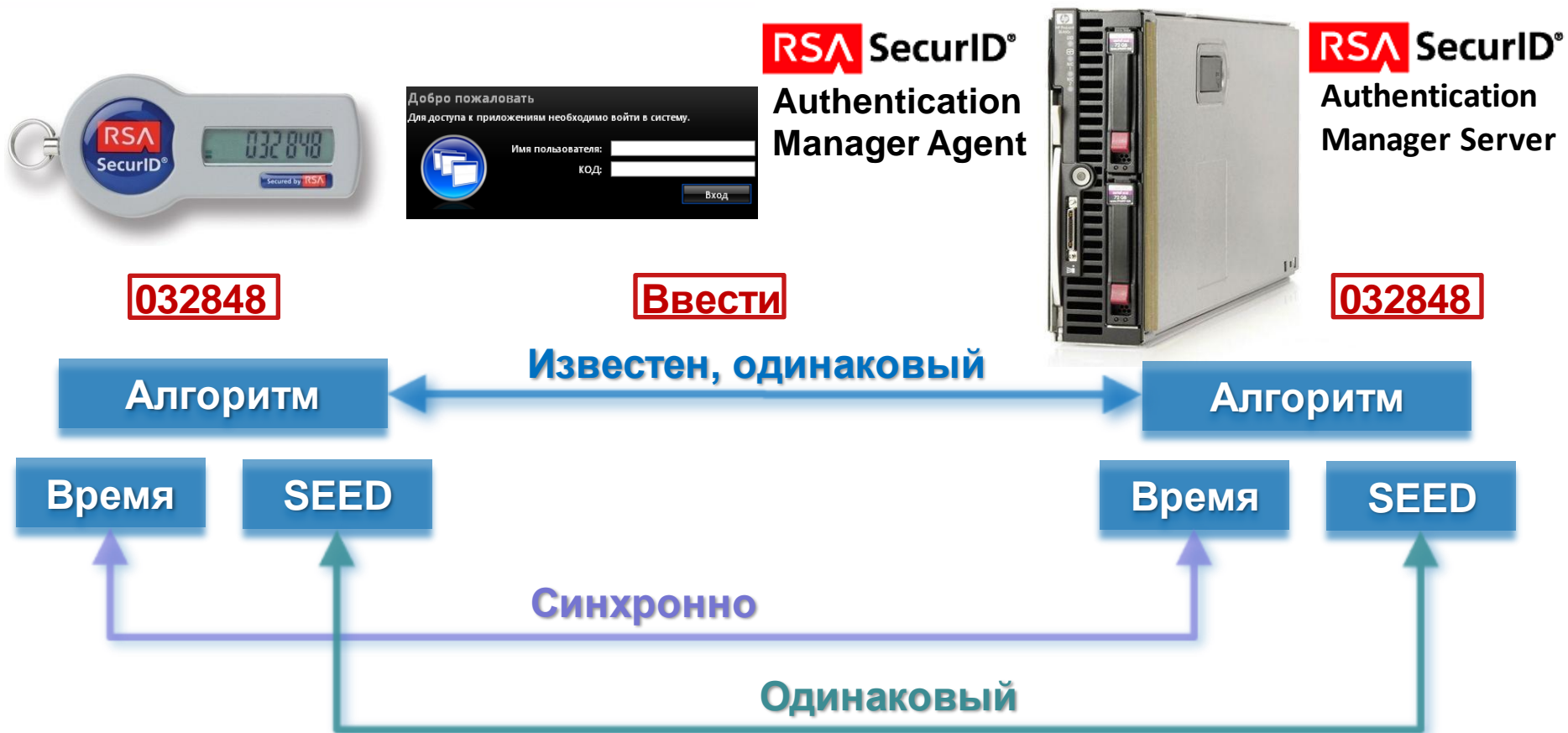
Пароль



Слабо

Сильно

Принципиальная схема работы системы RSA SecurID® Authentication Manager



Применение двухфакторной аутентификации RSA SecureID



И множество дополнительных возможностей, число которых растет с появлением новых версий продукта!

Компонент, обеспечивающий оптимизацию подсистемы печати

✓ **ThinPrint .print Application Server Engine**



Модель терминальной среды (Server Based Computing):

Сервер

ПК / тонкий клиент

Данные печати
создаются на
сервере



Задание печати

100 Mbps

DSL 1024 kbps

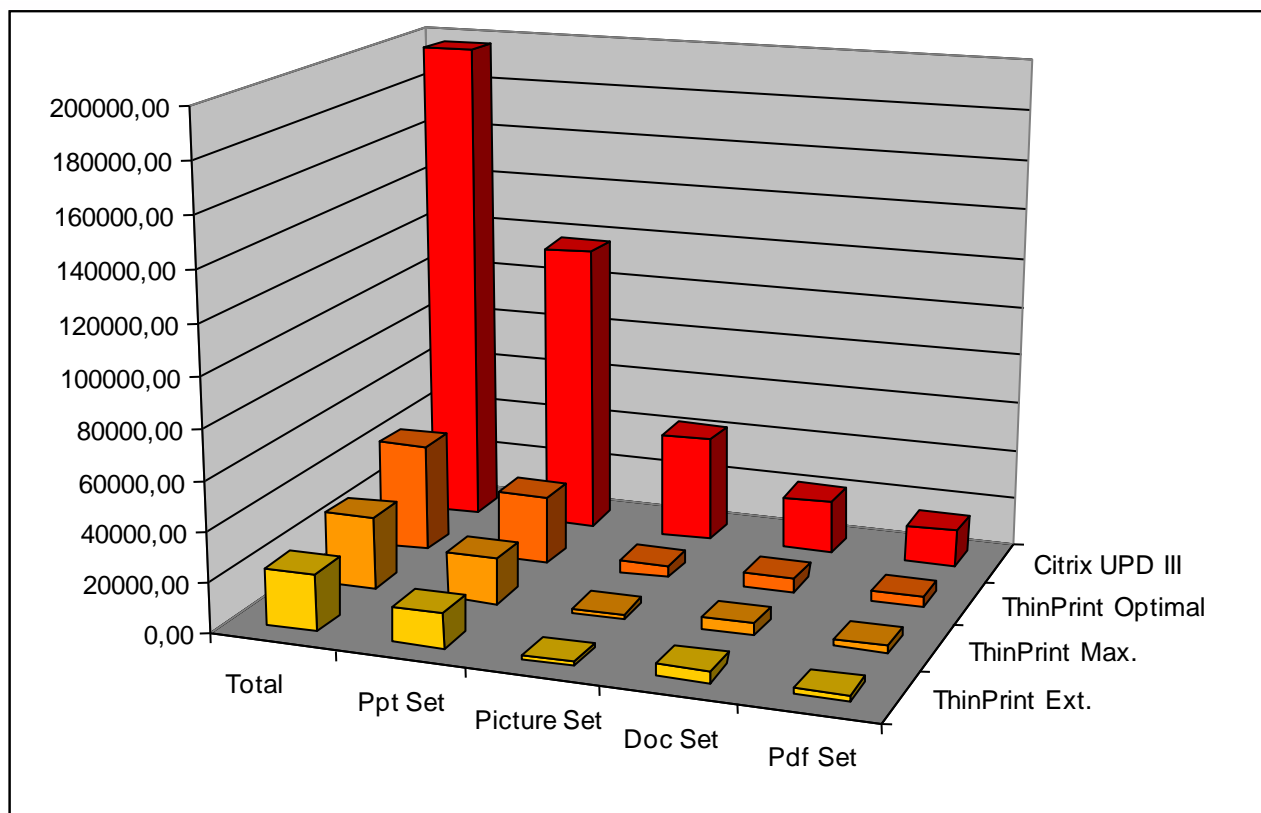
Session: 40 kbps

Наилучший способ обеспечить качественную печать



- ✓ DRIVER FREE PRINTING;
- ✓ Virtual channel tunneling;
- ✓ **Контроль полосы пропускания** в зависимости от соединения;
- ✓ **Сжатие** заданий печати;
- ✓ Автоматический маппинг принтеров ;
- ✓ **Сбалансированная** печать;
- ✓ Поддержка сетевых принтеров: TCP/IP, LPD;
- ✓ **Поддержка кластеров!**

Сравнение объема задач печати ThinPrint .print и CITRIX UPD 3:



ThinPrint .print для окружений Citrix это всегда оптимальное решение:

- ✓ **Независимость от платформы;**
- ✓ **Надежность и стабильность;**
- ✓ **Масштабируемость;**
- ✓ **Лёгкая интеграция;**
- ✓ **Эффективное использование полосы пропускания;**
- ✓ **Экономия на трафике благодаря высокому сжатию!**

ThinPrint[®]

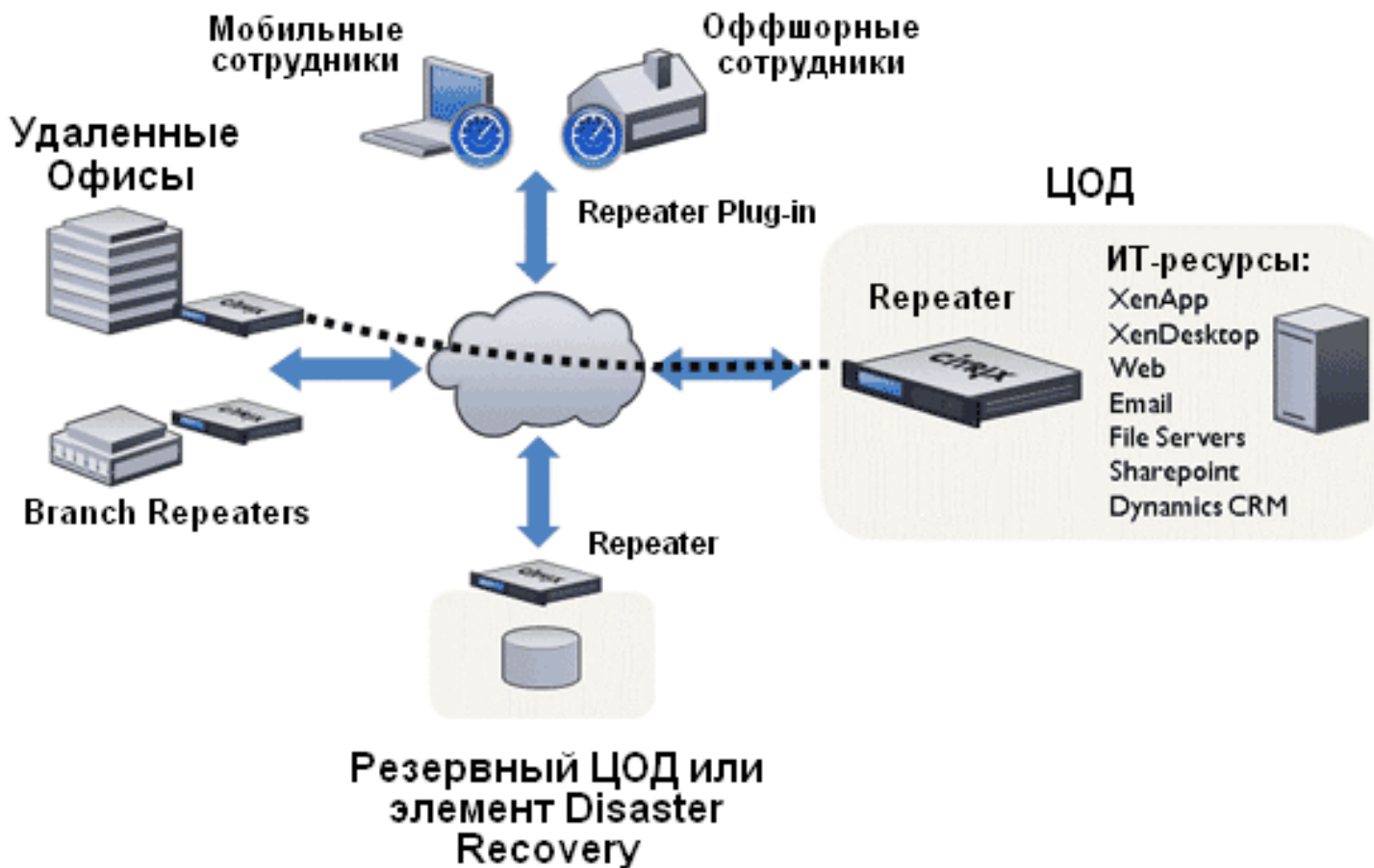


Компонент оптимизации узких каналов доступа к ресурсам

✓ **CITRIX Branch Repeater** (ранее известный как **WanScaler**)



Схема внедрения CITRIX Branch Repeater

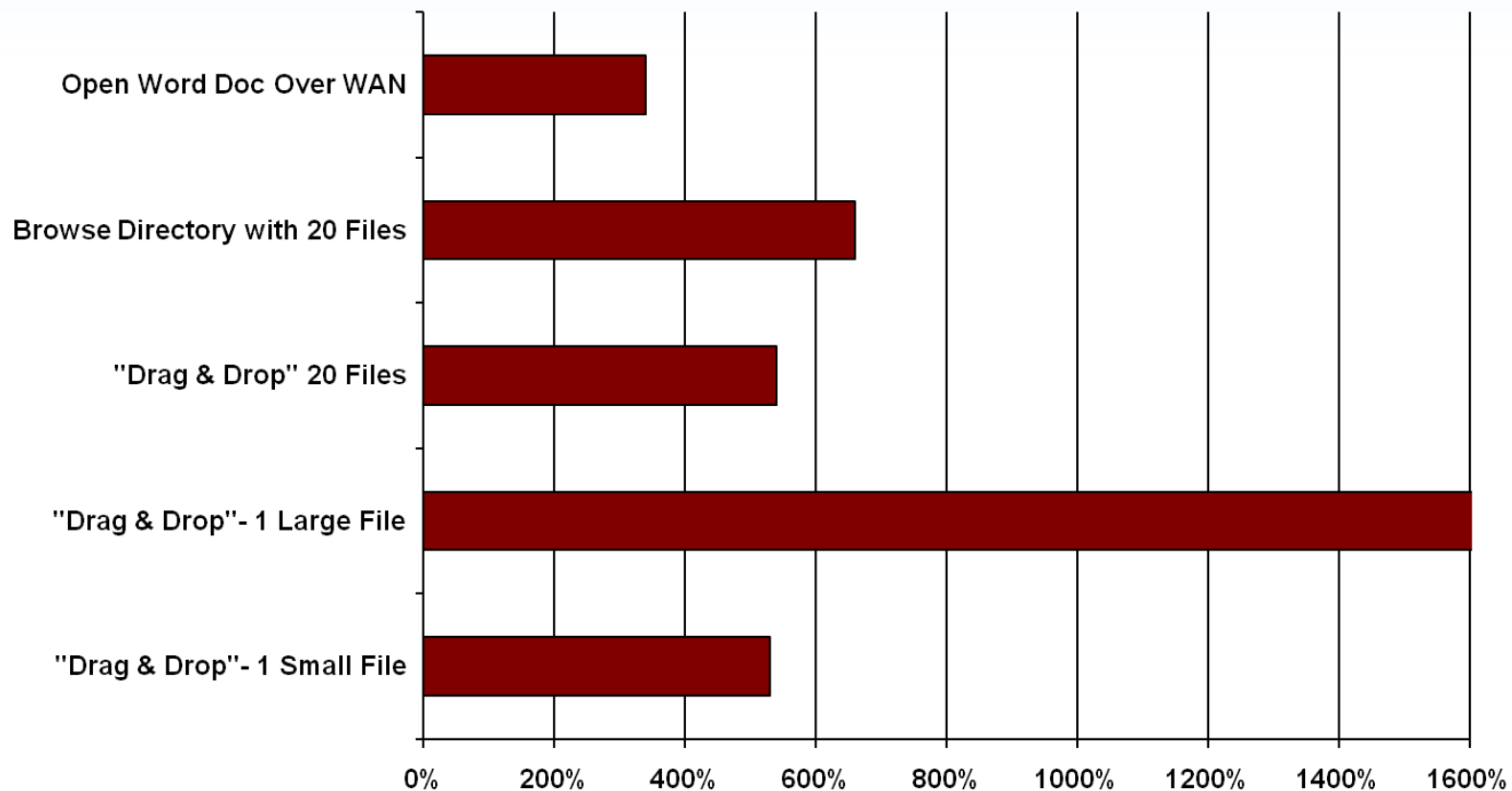


Компрессия

- ✓ Алгоритм компрессии выбирается динамически;
Выбор основан на динамике данных и скорости WAN канала
Никакого участия пользователя
- ✓ Citrix Repeater не оперирует на уровне файлов;
Оперирует с битовым потоком TCP
Никаких объектов, не зависит от приложений и протоколов
- ✓ Методы определения устаревших данных разнообразны;
- ✓ Зашифрованный трафик не подвергается компрессии;
- ✓ Средний показатель сжатия составляет 3:1.



Некоторые результаты оптимизации WAN-канала



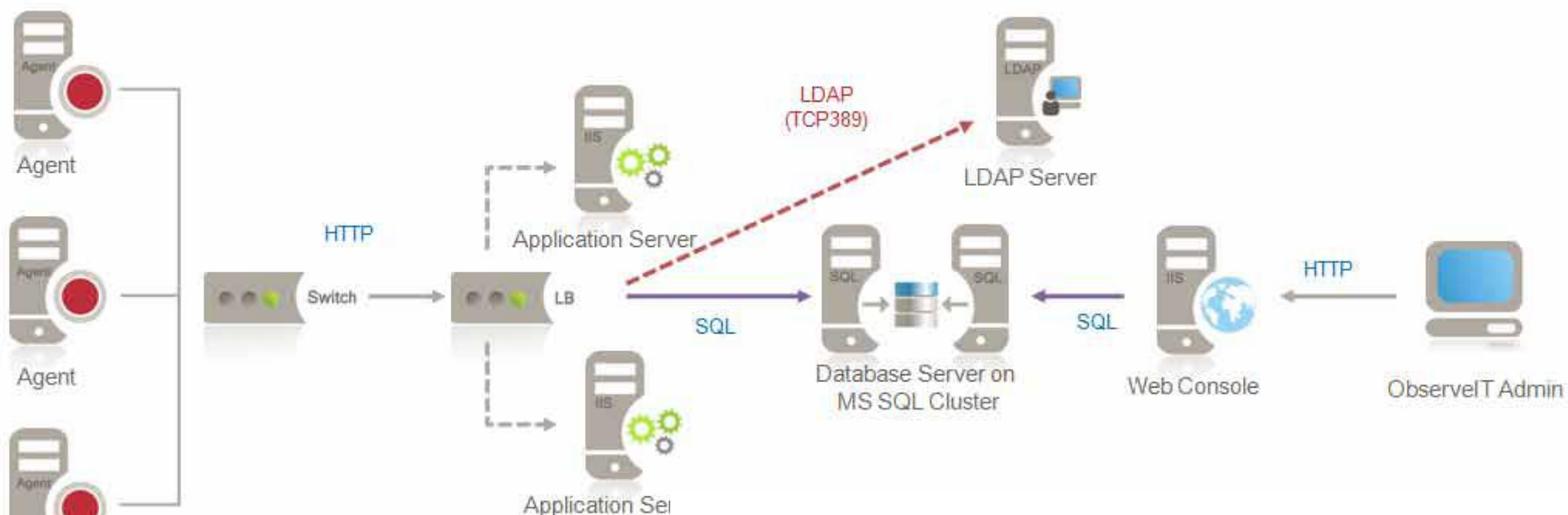
Улучшение времени ответа приложения

Уникальный компонент аудита активности пользователей системы

✓ **Observe IT**

observe **it**
People audit

Архитектура решения Observe IT

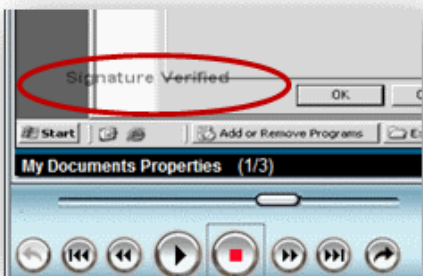


observe it
People audit

Observe IT – подробный аудит действий пользователей системы

- ✓ **Видеозапись сессии;**
- ✓ **Real Time оповещение ответственных лиц о совершении запрещенных действий, заданных фильтрами (например, выполнение команд: telnet, mstsc, ftp и др.);**
- ✓ **KeyStroke журналирование действий пользователя;**
- ✓ **Подготовка и просмотр отчетов по запрещенным**

действиям пользователей.



Компонент грануляции и контроля доступа пользователей

✓ **Xceedium GateKeeper**

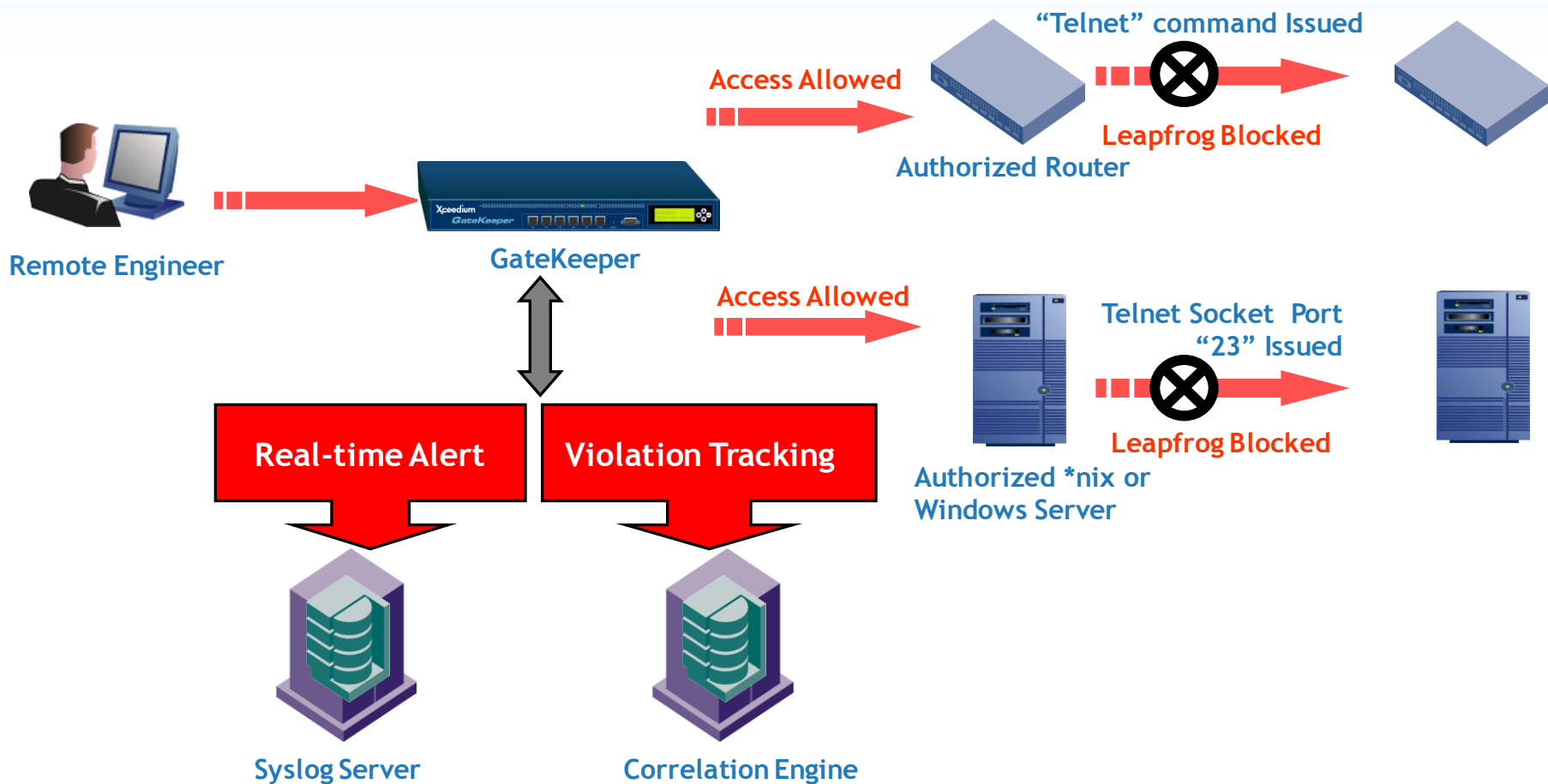


Уникальное управление правами доступа

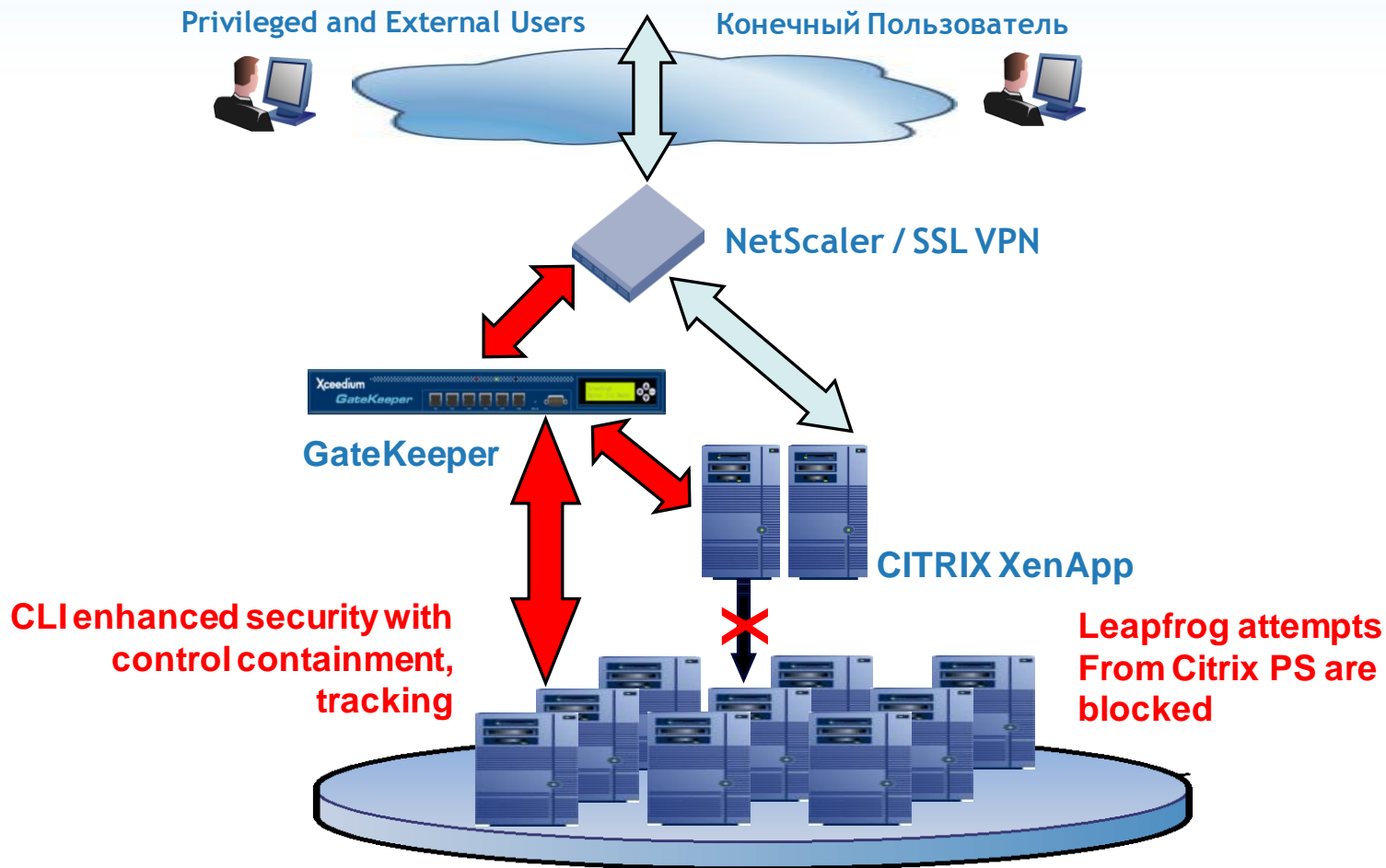
- ✓ Контроль за безопасностью критически важных сегментов ИТ-инфраструктуры;
- ✓ Принудительное применение гранулированных политик доступа;
- ✓ Мониторинг активности пользователей;
- ✓ Подготовка и просмотр отчетов по действиям пользователей и событиям в Системе!



Патентованная система LeapFrog



Краткая схема работы системы Xseedium Gatekeeper с CITRIX XenApp

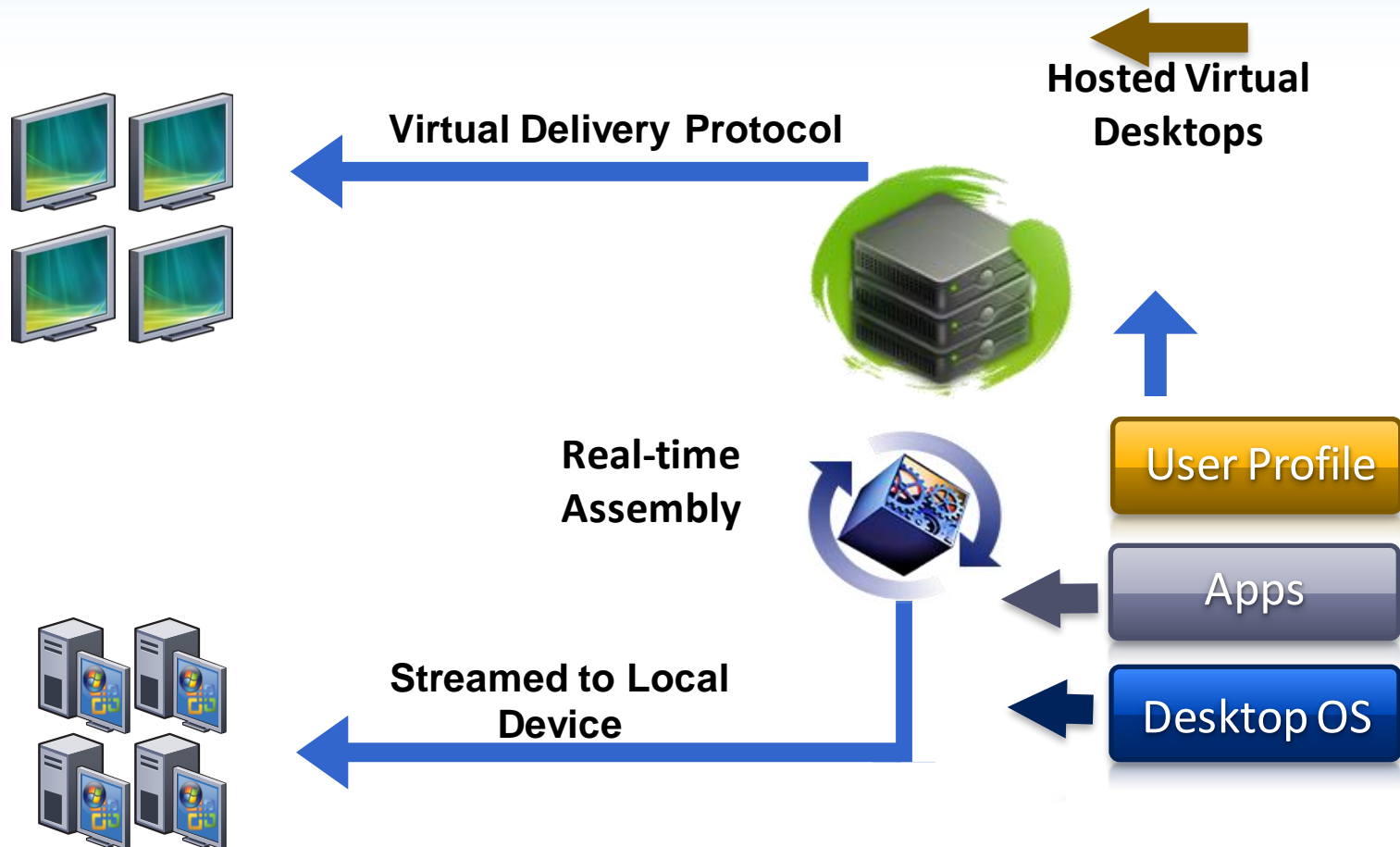


Компонент доступа к виртуальным рабочим станциям

✓ **CITRIX XenDesktop**



Краткая архитектура решения на основе CITRIX XenDesktop



Комплексное решение с применением всего комплекса опций

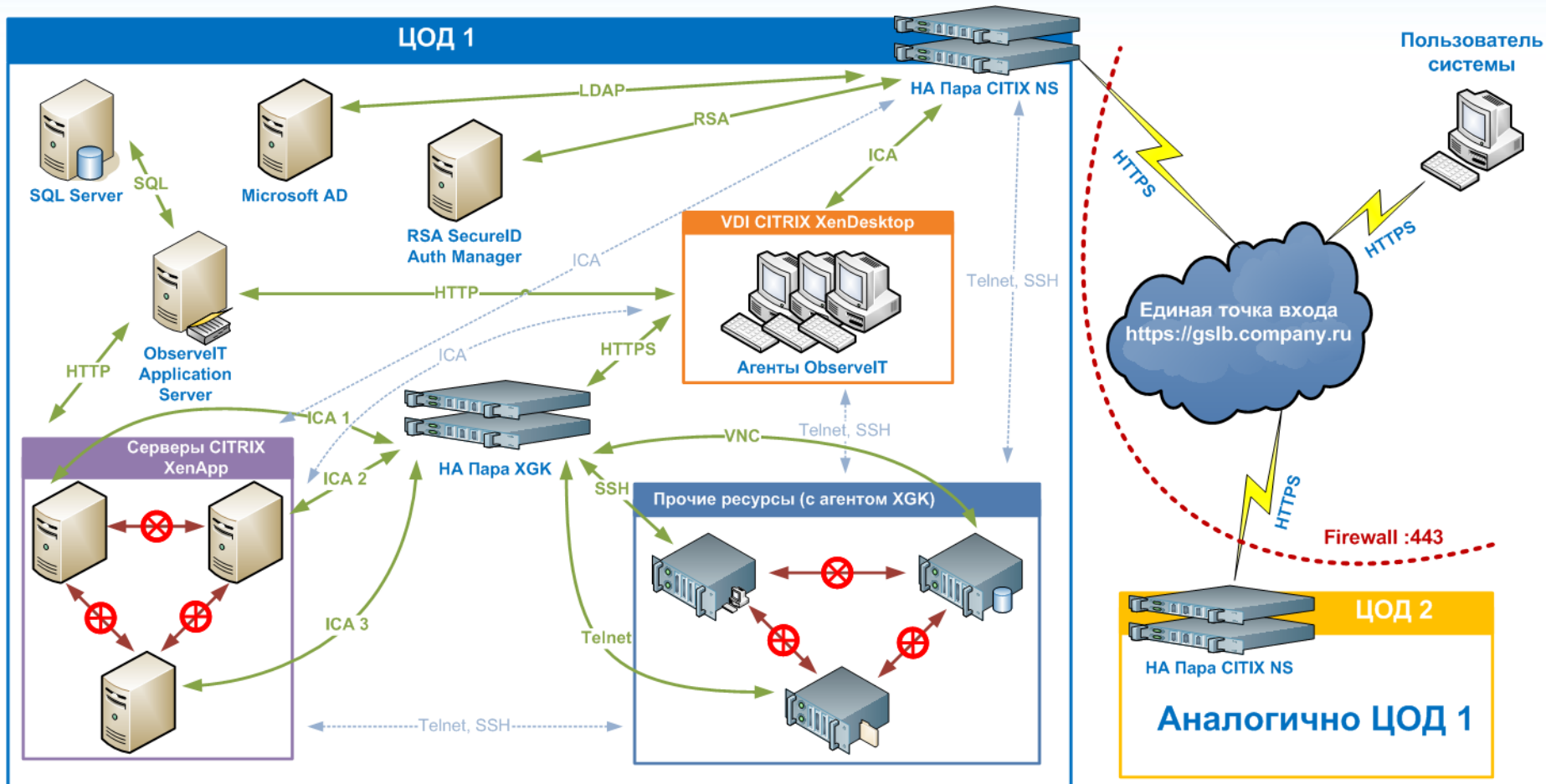
✓ **Комплексная** схема доступа на базе продуктов **CITRIX NetScaler** и **CITRIX XenApp** с применением дополнительных компонентов – **Observe IT**, **CITRIX XenDesktop**, **Xceedium GateKeeper**, **RSA SecurID**



observe **it**
People audit



Архитектура комплексного решения





Спасибо за внимание!



observe **it**
People audit

Миронов Дмитрий
mironov@complete.ru