



Quest[®]

Where Next Meets Now.

**Решения QUEST, о
которых вы знали
мало...**

Сергей Бобров | Quest, xBU





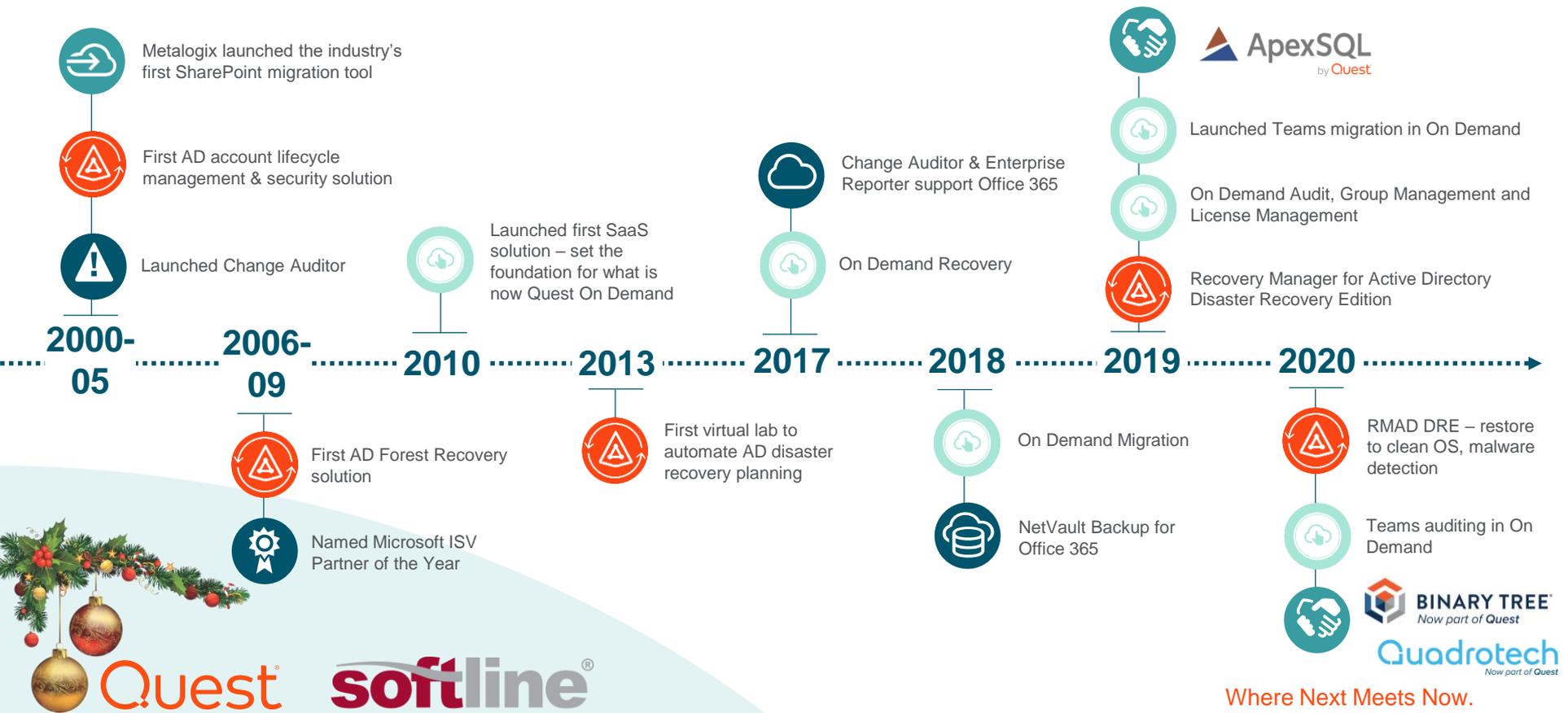
Мария Третьякова



Сергей Бобров

Quest CIS team

Покоряем будущее в течение 20 лет



Предпосылки угроз безопасности

Microsoft Active Directory, Exchange, SharePoint, Windows File Servers, VMware, NetApp, EMC и SQL Server являются частью вашей критичной инфраструктуры

- Аудит изменений и история событий – обязательное требование для безопасности инфраструктуры
- Нет всеобъемлющего анализа изменений и событий, так как данные лежат в разных локациях и форматах
- Поиск отдельного события занимает много времени
- Нативные логи содержат слишком мало читабельной информации и много специфичеких данных, чтобы читать которые, требуется подготовка
- Нет защиты чувствительных данных от удаления или логов от перезаписи. Администраторы не в курсе событий, пока не станет слишком поздно, вызывая потенциальные простои и повышая риски.
- Создание репортов занимает очень много времени
- Если рассматривать отдельное событие в «эко-системе» MS, то детализация не достаточная

Security

Change Auditor

InTrust

Enterprise Reporter

Quest[®]
Where Next Meets Now.

softline[®]

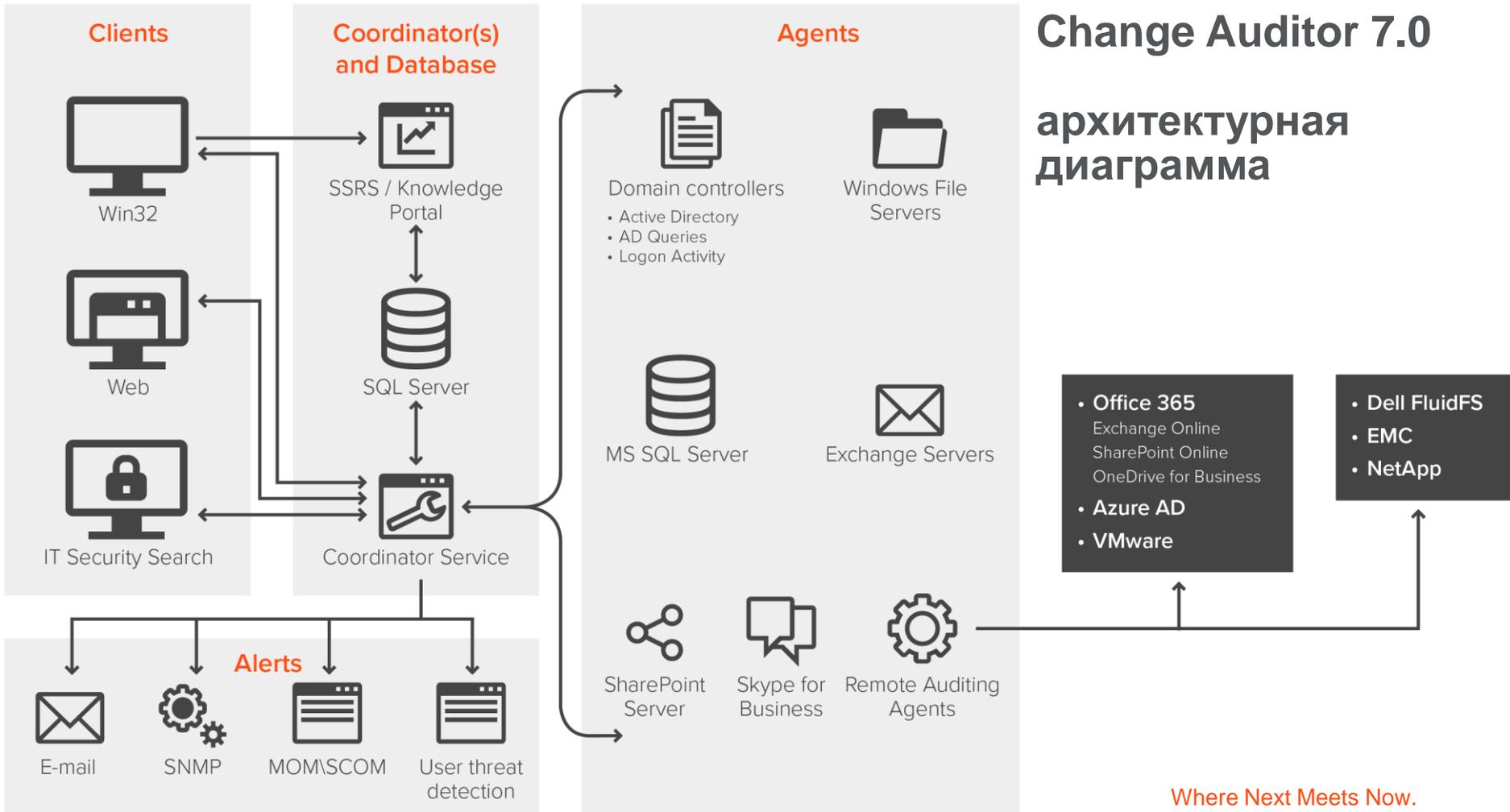
Change Auditor

- Change Auditor предоставляет полный, в реальном времени аудит всех пользовательских и административных изменений.



Change Auditor 7.0

архитектурная диаграмма



Where Next Meets Now.

Интерфейс

File Edit Action View Help

Overview | Searches

Overview Event Details Print

My Favorite Search: Change Auditor Real-Time

Run on: 5/19/2015 1:33 PM Run Time: 00:00:02
Next Refresh: 5/19/2015 1:38 PM Records: 696 Refresh

Drag a column header here to group by that column.

Severity	Time Detected	Subsystem	User	Event	Server	Action	Domain	Result
Medium	5/19/2015 1:32 PM	Active Directory	TITANCORP\barker	Office changed on user object	DC2	Modify A...	TITANCO...	Success
Medium	5/19/2015 1:32 PM	Active Directory	TITANCORP\barker	Office changed on user object	DC2	Add Attr...	TITANCO...	Success
Medium	5/19/2015 1:32 PM	SQL	TITANCORP\svcSharepoint	Audit Login Failed	SQL	Other	TITANCO...	None
Medium	5/19/2015 1:32 PM	SQL	TITANCORP\svcSharepoint	Audit Login Failed	SQL	Other	TITANCO...	None
Medium	5/19/2015 1:31 PM	SQL	TITANCORP\svcSharepoint	Audit Login Failed	SQL	Other	TITANCO...	None
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC1	Other	SITRAKA	Success
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC1	Other	SITRAKA	Success
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC1	Other	SITRAKA	Success
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC1	Other	SITRAKA	Success
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC1	Other	SITRAKA	Success
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC1	Other	SITRAKA	Success
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC1	Other	SITRAKA	Success
Medium	5/19/2015 1:31 PM	Logon Activity	SITRAKAWSQL_e05f365bd...	User authenticated through Kerberos	SWDC2	Other	SITRAKA	Success

Copy Email... Print Knowledge Base... Comments... Disable Related Search Restore Value

Medium Severity

Who: TITANCORP\barker (Shawn Barker) ← Кто сделал изменение

Where: DC2 ← Где оно было сделано

What: The office was changed from Chicago to New York for user cn=Lance Strewm,ou=Sbarker,OU=DSG Team OU,DC=titancorp,DC=local.

Active Directory Action: Modify Attribute

Class: user

Object: titancorp.local/DSG Team OU/Sbarker/Lance Strewm

From: Chicago ← Какой объект был изменен

To: New York ← Значение до и после

When: 5/19/2015 1:32:26 PM ← Когда

Origin: mem1.titancorp.local (10.1.146...)

Result: Success

Facility: Custom User Monitoring

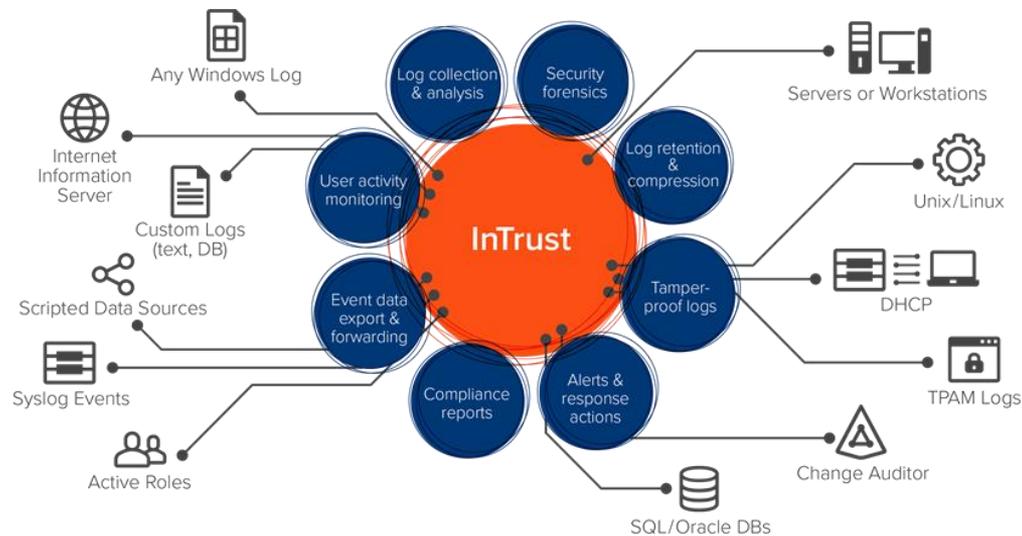
SSL/TLS: No

Sign/Seal: Yes

С какой рабочей станции

Менеджер логов InTrust

- Сбор, сжатие, поиск и анализ больших объемов данных
- Простота поиска по логам
- Единый интерфейс
- Результаты в реальном времени
- Расследование инцидентов в несколько кликов
- Выгодное хранение за счет использования сжатия



Enterprise Reporter

- Показывает данные - кто, где когда получал доступ к файлам или папкам по всей сети и на каком сервере.
- Добавляет визуализацию в процесс проверки настроек безопасности.
- Масштабируемая архитектура, поддержка больших инфраструктур и сложных Windows-окружений



IT Security Search

IT Security Search

September 1, 2015 - September 10, 2015
Administrator

Computers 2330
Events 3780
Files 2573
Groups 2568
OUs 27
Shares 47
Users 2976

Who:

- KNielsen 27449
- NHanders 7396
- MVilleneuve 5821
- SMughal 334
- ARoves 321
- Show 2 more

Workstation:

- MSP8456.amer.sitraka.com 27780
- YYZ8457.amer.sitraka.com 7400
- YYZ8458.amer.sitraka.com 5820
- GLA8459.amer.sitraka.com 22
- GLA8460.amer.sitraka.com 11
- Show 4 more

What:

- File deleted 17131
- Logon 11947
- Special Privileges assigned 11921
- Filtering Platform Connection 7024
- A user session took place 385
- Show 7 more

Where:

- MSP8456 27784
- YYZ8457 7774
- YYZ8458 7400
- GLA8459 5823
- GLA8460 477

Events timeline

Workstation: MSP8456.amer.sitraka.com | What: File deleted

Results found: 3780 Export

When	Who	Workstation	What	Where
09/01/2015 5:17 PM	KNielsen	MSP8456.amer.sitraka.com	A user session took place	MSP8456
09/02/2015 4:51 PM	NHanders	YYZ8457.amer.sitraka.com	File deleted	YYZ8457
09/03/2015 3:08 AM	MVilleneuve	YYZ8458.amer.sitraka.com	File deleted	YYZ8458
09/03/2015 5:28 PM	SMughal	GLA8459.amer.sitraka.com	A user session was ended by user stopping a terminal servi...	GLA8459
09/04/2015 11:29 AM	ARoves	GLA8460.amer.sitraka.com	A user session took place	GLA8460
09/05/2015 12:01 AM	KChan	MSP8461.amer.sitraka.com	Logon	MSP8461
09/05/2015 6:24 AM	svc-mm2sp1287		Special Privileges assigned	E1EAA1MSPWEX/C01
09/05/2015 4:20 PM	svc-mm2sp1287		Special Privileges assigned	E1EAA1MSPWEX/C02
09/06/2015 2:38 PM	svc-mm2sp1287	GLA8462.amer.sitraka.com	Logon	GLA8462
09/07/2015 7:59 AM	svc-mm2sp1287		Special Privileges assigned	E1EAA1MSPWEX/C01
09/07/2015 6:56 PM	svc-mm2sp1287	YYZ8468.amer.sitraka.com	Logon	YYZ8468
09/08/2015 7:25 AM	svc-mm2sp1287		Special Privileges assigned	E1EAA1MSPWEX/C01
09/08/2015 10:18 AM	svc-mm2sp1287	YYZ8417.amer.sitraka.com	Logon	YYZ8417
09/09/2015 12:01 AM	svc-mm2sp1287		Special Privileges assigned	E1EAA1MSPWEX/C01



Where Next Meets Now.

IT Security Search

The screenshot displays the IT Security Search interface. At the top, a search bar contains the query: "Where:'SPB9240.PROD.QUEST.CORP' AND Path='D:\Images\jurkag\ACS PDO specs\PDO\lrr'". Below the search bar, navigation tabs include 'Computers 0', 'Events 0', 'Files 1', 'Groups 0', 'OUs 0', 'Shares 0', and 'Users 0'. The 'Files 1' tab is active, showing a breadcrumb path: 'Files > OpsMgr ACS_ Successful AD Administrator Logons.xml'. On the left, a file card for 'OpsMgr ACS_Succe...' is shown with its path: 'D:\Images\jurkag\ACS PDO'. Below the file card, metadata is listed: Computer (SPB9240.PROD.QUEST.CORP), Owner (SPB9240\Administrators), Size (29295 bytes), Type (File), Created (6/29/2010 9:51:11 AM), Last Accessed (7/23/2010 8:30:33 PM), and Last Modified (11/14/2008 2:27:57 PM). Under 'Actions', there are links for '> Who accessed this file' and '> Who changed permissions on this file'. On the right, the 'Permissions' tab is selected, displaying a table of permissions for the file.

Account	Access Type	Permissions	Inheritance
NT AUTHORITY\SYSTEM	Allow	Full control	Inherited
SPB9240\Administrators	Allow	Full control	Explicit
SPB9240\Administrators	Allow	Full control	Inherited
SPB9240\auto	Allow	Read and execute Synchronize	Inherited
SPB9240\Remote Desktop Users	Allow	Modify Synchronize	Inherited
SPB9240\Users	Allow	Read and execute Synchronize	Inherited

Перерыв 5 минут!



Quest

softline®

Where Next Meets Now.

Решения миграции

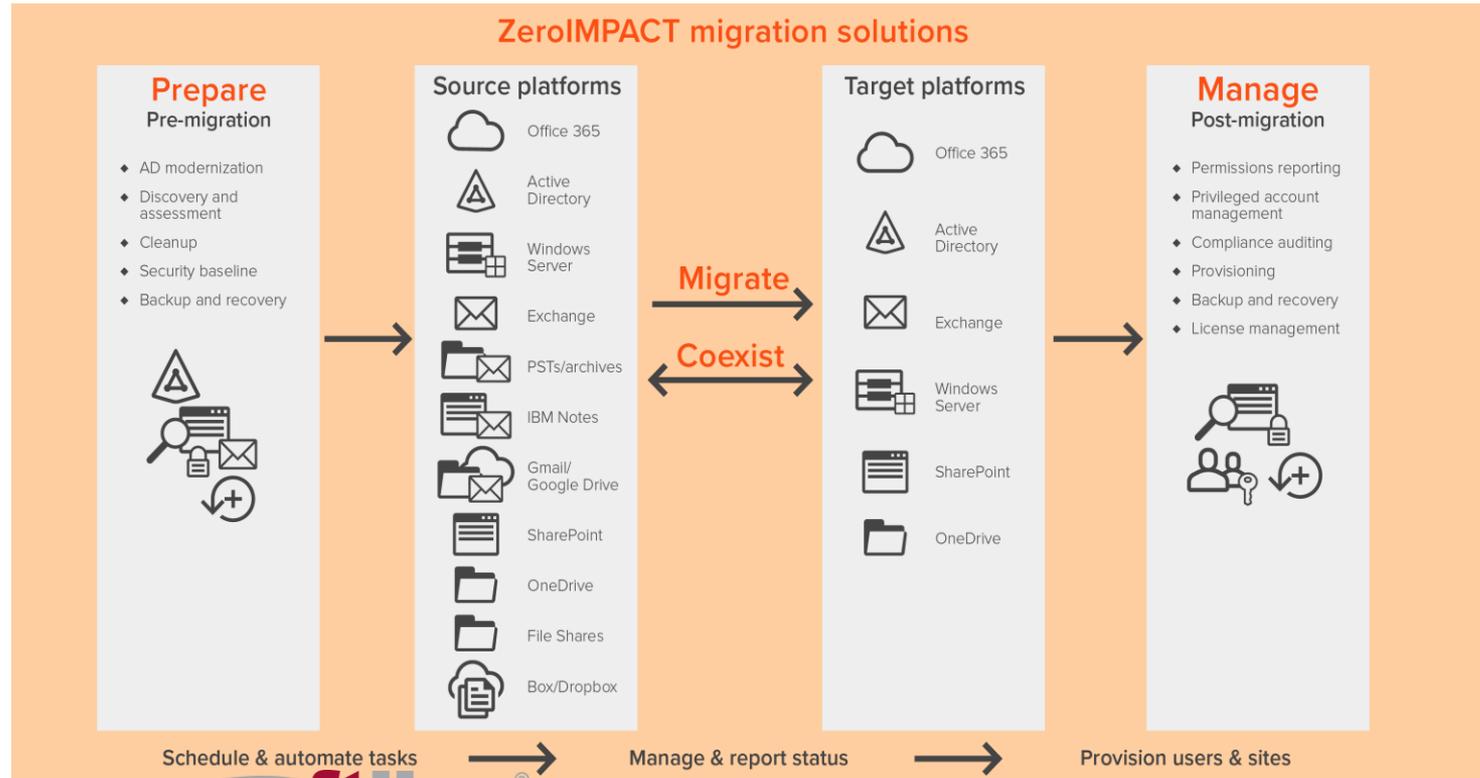
В среде MS и не только

Quest

softline®

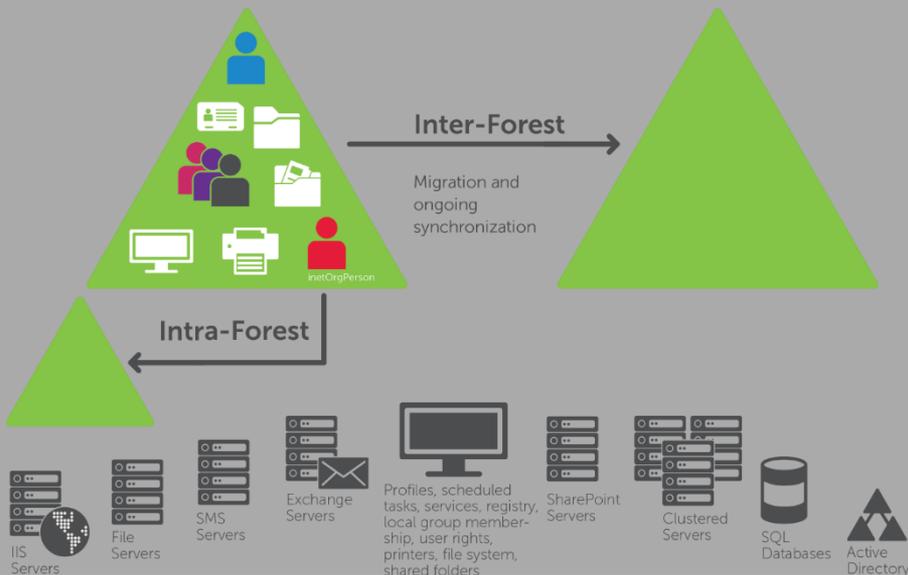
Where Next Meets Now.

Решения по миграции

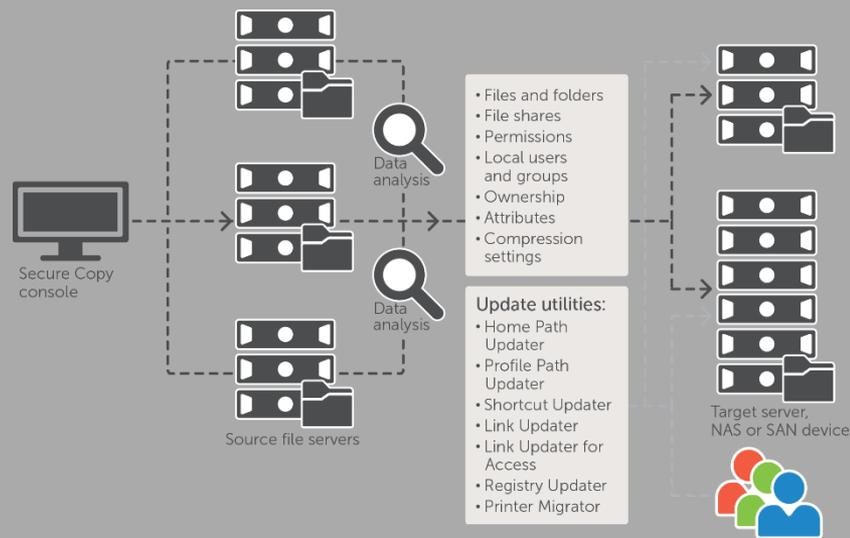


Migration Manager для AD & File Servers

Migration Manager для AD: Юзеры, PC, сервера, права доступа и другое

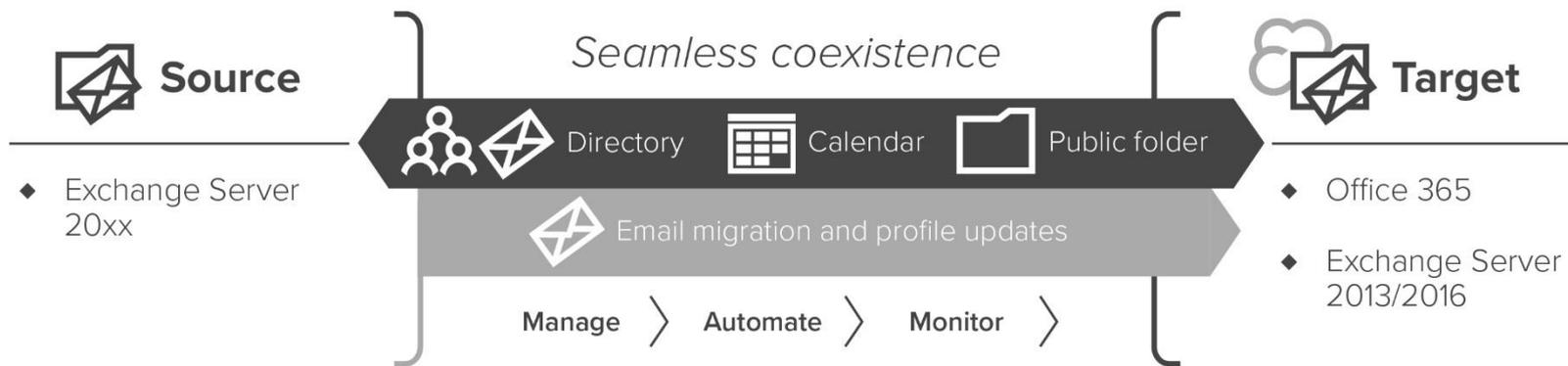


Secure Copy: файлы, папки, принтера, шары, NTFS security



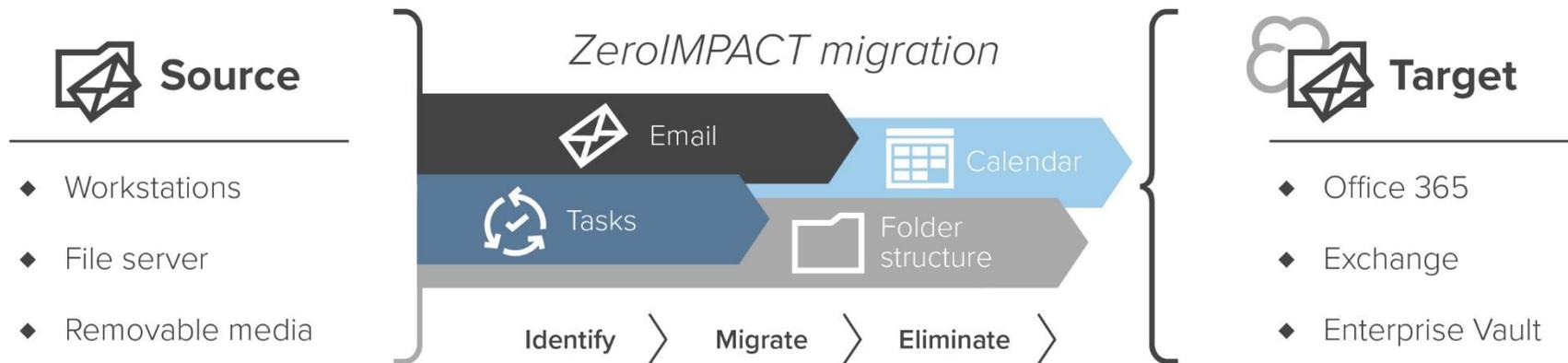
Migration Manager для Exchange

ZeroIMPACT Exchange Migration



Migration Manager для PSTs

Migration Manager for PSTs



OnDemand Migration для Email



Source
platforms

- Exchange
- Google Gmail
- IBM Notes
- GroupWise
- POP/IMAP
- Office 365
- Zimbra
- Sun ONE/iPlanet

ZeroIMPACT Migration

Powered by
Windows Azure



Manage > Migrate > Preserve >

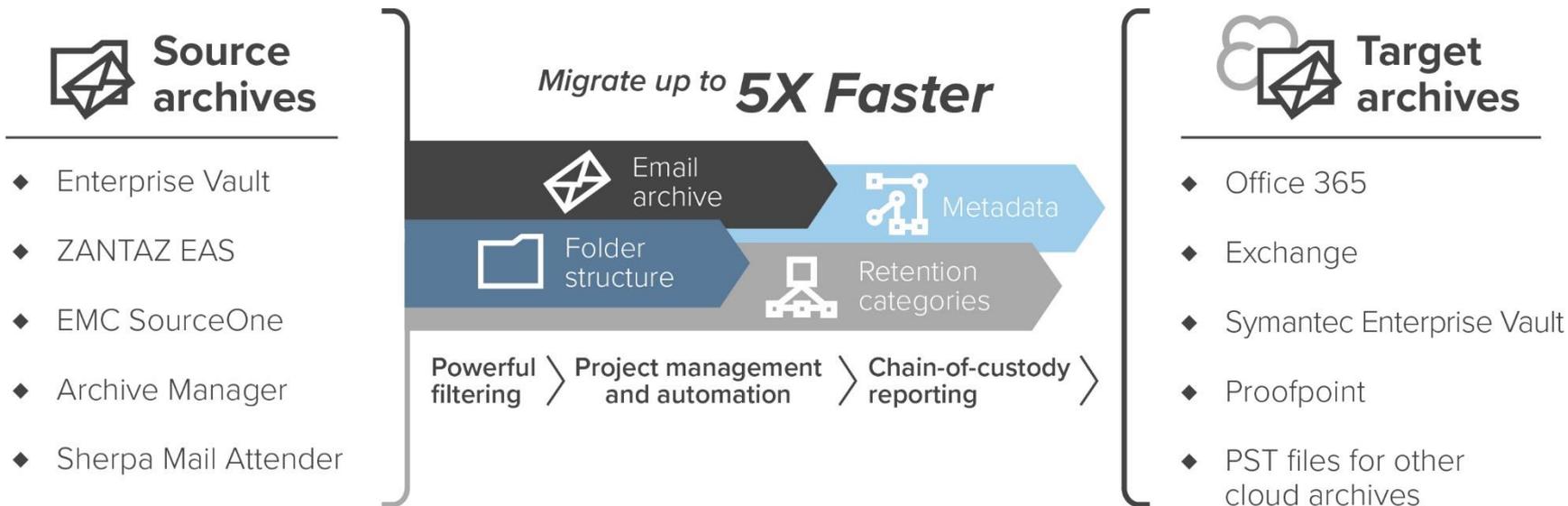


Target
platforms

- Office 365
- Exchange 2010/2013/2016
- Hosted Exchange

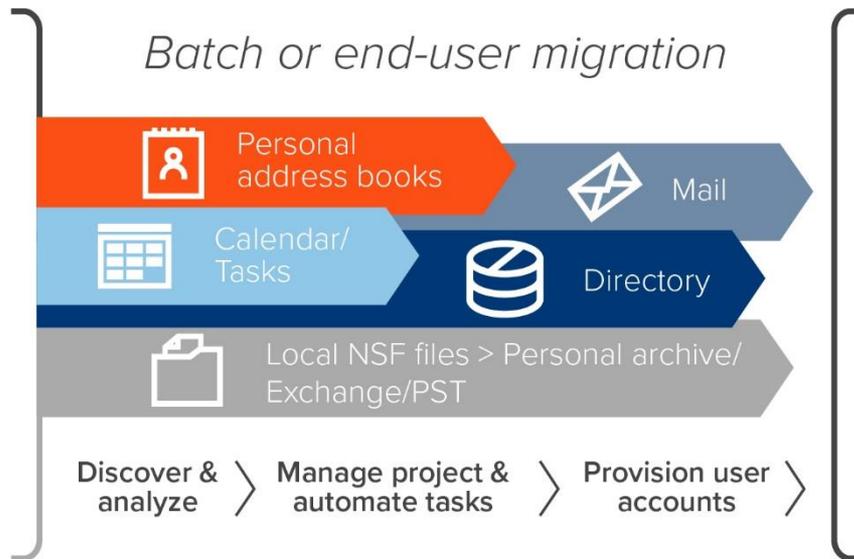
Migration Manager для Email Archives

ZeroIMPACT email archive migration



Migrator для Notes в Exchange

Comprehensive migration



Coexistence Manager для Notes

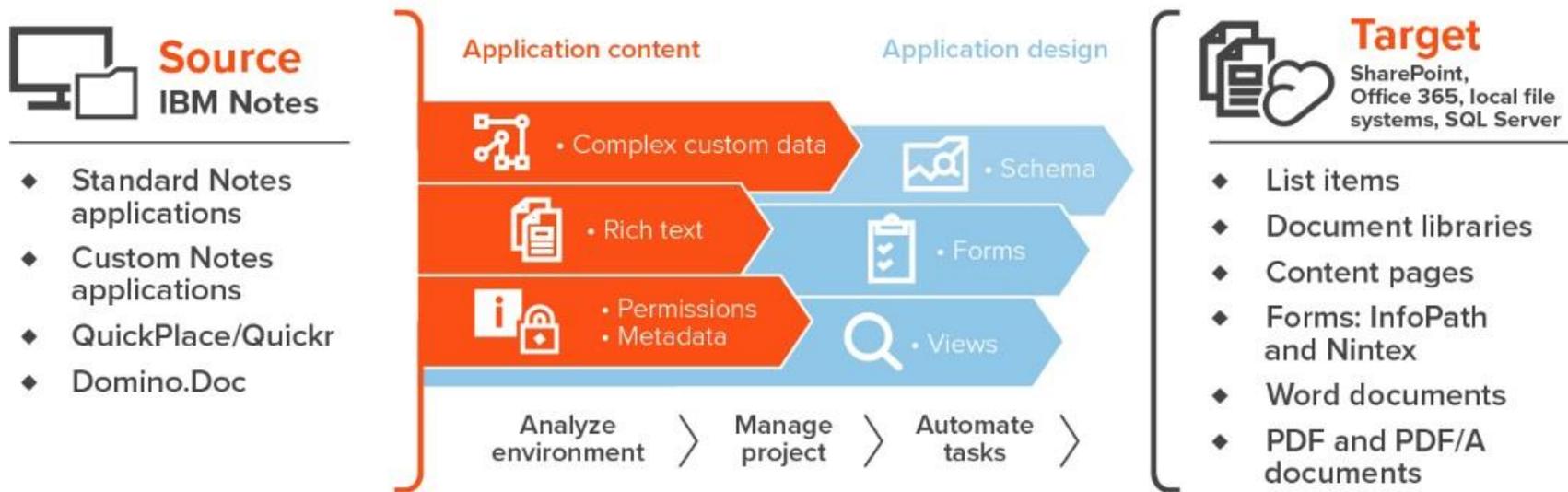
Coexistence Manager for Notes



Migrator для Notes в SharePoint

Command your Notes migration

Migrate or archive with high fidelity



Quest



BINARY TREE
Now part of Quest

Quest + Binary Tree =

лидирующая позиция на рынке
Microsoft Modernization



Учитывая доминирующее положение Quest в сфере слияний и поглощений, приобретение Binary Tree определенно станет отличным дополнением к их портфелю. Это усилит их влияние на миграцию от заказчика к заказчику.”

- Paul Caron, IT Manager, MaineHealth



Исходя из моего опыта, Quest всегда был лидером в предоставлении точных инструментов, которые заполняют пробел между продуктами Microsoft (и других) и собственной разработкой. С приобретением ВТ я ожидаю не что иное, как передовые технологии.”

- Jim Cochran, IT Security Manager, North America, Avnet

Quest

softline®

quest.com | confidential

Where Next Meets Now.

Что такое Binary Tree?

60m 

Юзеров мигрировано

15m



Юзеров мигр-но в Office 365

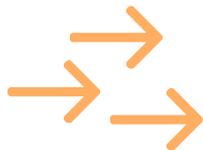
>5k



Средний размер заказчика

12k

Компаний трансформировано



2k

Слияний и поглощений



“ Чтобы перейти на новую Active Directory, нам пришлось провести то, что я назвал «операцией на открытом сердце» на 60 производственных площадках по всему миру. При поддержке Binary Tree мы достигли нашей цели в срок и в рамках бюджета, без проблем или незапланированных простоев. Я смог доложить руководству, что проект был успешным. ”

- Kay Matthiesen, Director of Global Infrastructure for YFAI

Решения для интеграции

Наше ПО для сосуществования позволяет работать пользователям разных SaaS окружений

Office 365 Tenants
Unified GAL, Free-Busy & Email Domain



Power365® Tenant-to-Tenant



Office 365 Tenants
Unified GAL, Free-Busy & Email Domain

Azure Active Directory



Power365® Directory Sync



Azure Active Directory

Active Directory



Active Directory

Active Directory



Directory Sync Pro



Active Directory

Domino Directory



Domino Directory
и Messaging



Notes Integration CMT



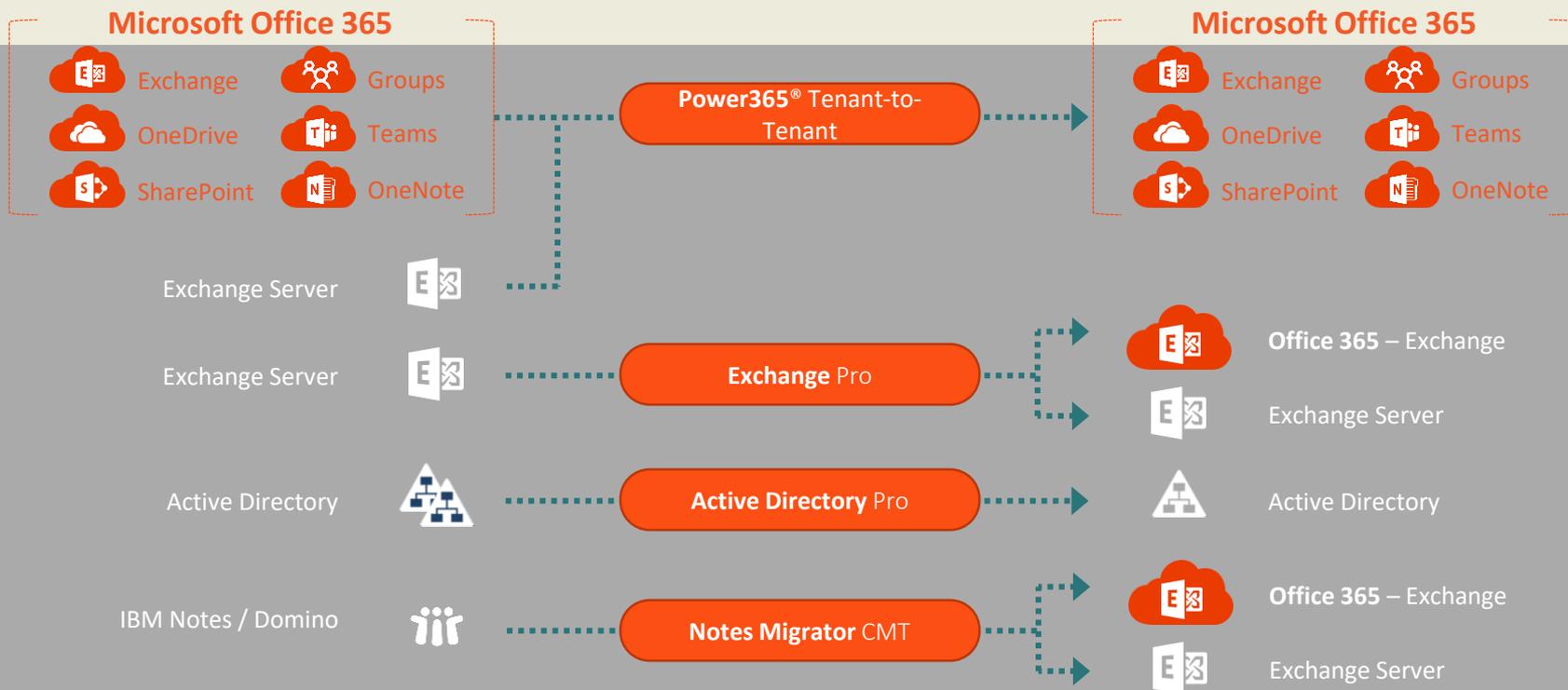
Azure Active Directory и
Exchange in Office 365



Active Directory и Exchange
Messaging

Решения для миграции

С помощью нашего решения на новые платформы мигрировало более 52млн пользователей.



THE POWER365® PLATFORM

POWERED BY BINARY TREE(QUEST)

Платформа трансформации в облако
enterprise уровня для Microsoft Office 365



Multi-Tenant Integration



Unified Email Domain



Unified Calendar Lookups



Unified Global Address List

On-Premises to Tenant Integration



Azure and On-Premises AD Integration



Password Sync for On-Premises AD

Multi-Tenant Migration



Exchange



Groups



OneDrive



Teams



SharePoint



OneNote

On-Premises to Tenant Migration



Exchange

Where Next Meets Now.

Quest

Quest | Quadrotech

Now part of Quest

Quest + Quadrotech =

укрепление позиций в области управления и миграции в/из Office 365 при росте числа пользователей



Эти две группы продуктов представляют собой лучшие инструменты в нескольких категориях. Мы уже несколько лет используем технологии Quadrotech и Quest для разных целей и очень рады видеть, как конвергенция этих инструментов поможет нам лучше поддерживать наших клиентов.”

- Stephen Revel, Senior Managing Architect, Insight



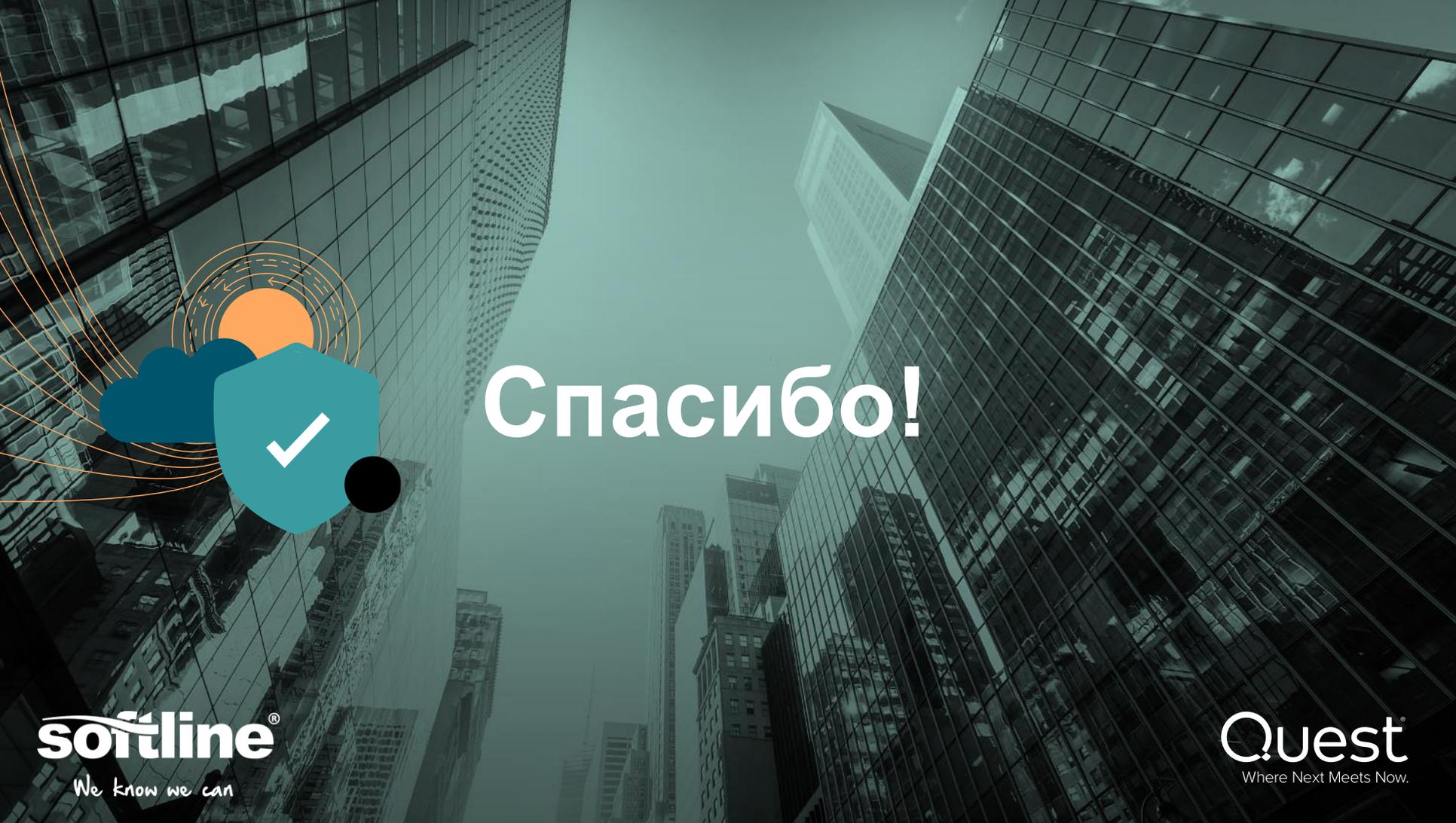
По моему опыту, Quest, кажется, чрезвычайно взвешен в своих приобретениях, стараясь сосредоточиться только на лучших инструментах для своих клиентов. Я уверен как менеджер и как администратор, что компания Quest тщательно проверила приобретённые инструменты на предмет функциональности, простоты внедрения и рентабельности инвестиций.”

- Jim Cochran, IT Security Manager, North America, Avnet

Quest **softline**[®]

quest.com | confidential

Where Next Meets Now.



Спасибо!

softline[®]
We know we can

Quest
Where Next Meets Now.