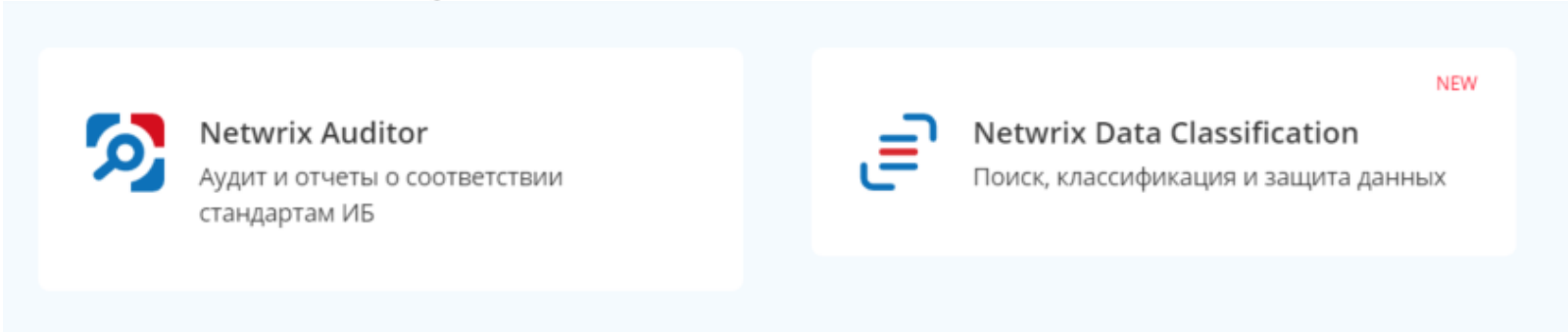
"Безопасность конфиденциальных данных с помощью решений Netwrix"

6 декабря (пятница), 11:00 – 12:30 (МСК)



Хиженков Владимир
RRC Россия | Руководитель проектов
khizhenkov_v@rrcgroup.com
Тел.: +7-495-956-1717 (#1099)
Факс: +7-499-133-5230 | www.rrc.ru

О компании Netwrix Corporation

1. Общие сведения о компании Netwrix
2. Ключевые изменения платформы
3. Эволюция платформы
4. Список решений
5. Истории успеха
6. Портал историй успеха
7. Обновления платформы, релизы, сроки выходов
8. Маркетинговые материалы
9. Образцы документации для конкурсов
10. Техническая поддержка
11. Партнерская программа
12. Защита сделки
13. Техническая поддержка

О компании Netwrix Corporation

Факты и цифры

2006 год основания

Головной офис:
Irvine, California, США

Более **250 сотрудников**
в США, России и Европе

Около **8000 заказчиков**
в 100 странах мира

Удовлетворенность клиентов 97%

С момента основания компания Netwrix удостоена **более 100 отраслевых наград**, а также включена в списки **самых быстрорастущих компаний**: Inc. 5000 и Deloitte Technology Fast 500 lists.

Redmond READER'S CHOICE AWARDS 2015 GOLD

Deloitte. Technology Fast 500

Redmond READER'S CHOICE AWARDS 2015 PLATINUM

Info Security Products Guide 2015 GLOBAL EXCELLENCE AWARDS

Inc. 5000 #2333 2015

SC MAGAZINE AWARDS 2016 FINALIST Honored in the U.S.

Ключевые изменения Netwrix

2008 Netwrix Active Directory Change Reporter

- Предустановленные отчеты об изменениях
- Один администратор, небольшие среды

2011 Netwrix Change Reporter Suite

- Пакет отдельных продуктов для аудита изменений
- Отчеты и оповещения в режиме реального времени

2013 Netwrix Auditor 5.0

- Единая платформа аудита, поддерживающая 6 приложений
- Видеозапись действий привилегированных пользователей

2014 Netwrix Auditor 6.0 and 6.5

- Сводные графики изменений по всем системам
- Netwrix Auditor for SharePoint
- Контроль доступа

2015 Netwrix Auditor 7.0 (VEGA) & Netwrix Auditor 7.1

- Интерактивный поиск данных аудита
- Шаблоны отчетов по ИБ стандартам
- Разграничение доступа к данным аудита на основе ролей
- Расследование инцидентов
- Поддержка NetApp Clustered Data ONTAP

2016 Netwrix Auditor 8.0

- Netwrix Auditor for Office 365
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Файловый анализ
- RESTful API and Netwrix Auditor Add-on Store
- Поддержка виртуальных машин и облачных платформ

2017 Netwrix Auditor 9.0

- Уведомления об угрозах безопасности
- Add-on for Cisco
- Управление доступом на основе ролей
- Отчеты для стандартов: GDPR, CJIS, FERPA, NERC CIP, GLBA

2016 Netwrix Auditor 8.5

- Netwrix Auditor for Azure AD
- Netwrix Auditor for Oracle Database
- Анализ действий пользователей
- Новые возможности интеграции с SIEM

2017 Netwrix Auditor 9.5

- Оценка рисков
- Обнаружение подозрительных действий
- State-in-Time отчеты для Windows Server
- Add-on for ServiceNow Incident Management
- Add-on for Generic Linux Syslog
- Add-on for Privileged User Monitoring on Linux and Unix Systems

2018 Netwrix Auditor 9.6

- Data discovery and classification for Windows file servers
- Data discovery and classification for Dell EMC storage devices
- Data discovery and classification for NetApp filers

Истории успеха

Netwrix Customer Case Study

UzKDB Bank

Аудит изменений IT-инфраструктуры: как обеспечить выполнение требований норматива PCI DSS

Аудит изменений IT-инфраструктуры: как обеспечить выполнение требований норматива PCI DSS

«UzKDB» Банк является одним из лидирующих банков Узбекистана, оказывающим широкий спектр банковских услуг, включая обслуживание частных и корпоративных клиентов, инвестиционный банковский бизнес, торговое финансирование и управление активами.

Для успешной работы на рынке банку необходимо обеспечить соответствие IT-инфраструктуры требованиям стандартов информационной безопасности, а именно PCI DSS. Зная, что подготовка необходимой документации вручную отнимает большое количество времени, начальник IT-отдела Дмитрий Некрасов обратился к поиску соответствующих программных решений, позволяющих упростить процедуру прохождения сертификации.

ЗАКАЗЧИК
ЗАО «UzKDB» банк

САЙТ
www.kdb.uz

ОТРАСЛЬ
Банки и финансы

РЕШЕНИЕ
Аудит изменений и управление доступом

ПРОДУКТ
Netwrix All-in-One Suite

ПРОФИЛЬ
UzKDB банк – универсальный банк, осуществляющий основные виды банков-ских операций, представленных на рынке финансовых услуг, включая обслуживание частных и корпоративных клиентов, инвестиционный банковский бизнес, торговое финансирование и управление активами.

"Netwrix All-in-One Suite позволил решить вопросы единого средства мониторинга активности пользователей и сбора журнала событий с определённого числа компьютеров и серверов. При его наличии мы уверены в прохождении сертификации PCI DSS".

Дмитрий Некрасов,
Начальник IT-отдела , UzKDB Банк

Netwrix Customer Case Study

Ломбарды ювелирной сети 585 используют Netwrix Auditor для отслеживания изменений в ИТ-инфраструктуре

Компания Netwrix поставила лицензию на 1700 учетных записей для программного обеспечения Netwrix Auditor в сеть ломбардов «ЗОЛОТОЙ/585» (ГК «Ювелирная сеть Золотой/Gold 585», Компания 585). Решение позволило контролировать ИТ-инфраструктуру в онлайн режиме и оперативно решать возникающие инциденты.

ЗАКАЗЧИК
Всероссийская сеть ломбардов «ЗОЛОТОЙ»

САЙТ
http://www.zolotoylom.ru/

ОТРАСЛЬ
Розничная торговля

РЕШЕНИЕ
Контроль изменений

ПРОДУКТ
Netwrix Auditor

ПРОФИЛЬ
Всероссийская сеть ломбардов «ЗОЛОТОЙ/585» - является крупнейшей сетью ломбардов в России. Компания работает в 120 городах РФ и насчитывает более 410 ломбардов.

"Netwrix Auditor очень прост в управлении, все действия выполняются из одной консоли. Безусловным преимущество ПО являются грамотно настроенные отчеты – они информативны и просты в восприятии. Внедрив данное ПО, мы обеспечили достойный уровень безопасности наших ИТ ресурсов – любые спорные ситуации или инциденты теперь решаются гораздо быстрее»

Антон Литвинов,
Начальник отдела техподдержки,

Истории успеха

Netwrix Customer Case Study

Компания Netwrix сообщает о завершении проекта по поставке 5000 лицензий программного продукта Netwrix Auditor, предназначенного для контроля изменений в Active Directory, групповых политиках и Microsoft Exchange – в ОАО «ТрансКонтейнер».

ЗАКАЗЧИК
Трансконтейнер (ЗАО)

САЙТ
www.trcont.ru

ОТРАСЛЬ
Грузовые перевозки

РЕШЕНИЕ
Контроль изменений в Active Directory

ПРОДУКТ
Netwrix Auditor

ПРОФИЛЬ

ОАО «ТрансКонтейнер» - ведущий российский оператор контейнерных интермодальных перевозок.

ТрансКонтейнер внедрил Netwrix Auditor для контроля изменений в инфраструктуре Microsoft

ОАО «ТрансКонтейнер» является ведущим российским оператором контейнерных интермодальных перевозок. Владея примерно 60% общего российского парка фитинговых платформ, Компания осуществляет 50% железнодорожных контейнерных перевозок и 30% переработки контейнеров на железнодорожных терминалах России. ОАО «ТрансКонтейнер» располагает 46 собственными терминалами во всех грузообразующих центрах России. Кроме того, ОАО «ТрансКонтейнер» является крупнейшим в России, странах СНГ и Балтии владельцем парка специализированного подвижного состава: в его собственности находится свыше 24 тыс. фитинговых платформ и около 60 тыс. крупнотоннажных контейнеров.

Netwrix Customer Case Study

Компания Netwrix успешно завершила проект внедрения Netwrix Active Directory Change Reporter (ADCR) в целях контроля ИТ-инфраструктуры Транскапиталбанка. Система обеспечивает оперативное выявление и реагирование на инциденты, возникающие в сфере информационной безопасности, что существенно повышает управляемость ИТ-инфраструктуры в целом.

ЗАКАЗЧИК
АКБ «ТРАНСКАПИТАЛБАНК» (ЗАО)

САЙТ
transcapital.com

ОТРАСЛЬ
Банки и финансы

РЕШЕНИЕ
Контроль инфраструктуры, аудит изменений AD, аудит изменений групповых политик

ПРОДУКТ
Netwrix Auditor – Activer Directory

ПРОФИЛЬ

Универсальный банк, выполняющий все основные виды финансовых операций. По размеру активов и уставного капитала Транскапиталбанк стабильно входит в 50 крупнейших российских банков.

Транскапиталбанк внедрил Netwrix Active Directory Change Reporter для контроля ИТ-инфраструктуры

Транскапиталбанк работает на рынке финансовых услуг с 1992 года и стабильно входит в ТОП-50 крупнейших и ТОП-30 самых надежных российских банков. В целях обеспечения безопасности хранения данных, Банк уделяет большое внимание защите своей ИТ-инфраструктуры с учетом принятых в финансовых системах стандартов ИБ.

«Проект по внедрению Netwrix Auditor оправдал наши ожидания. Теперь администраторы, работающие с AD, находятся в курсе всех изменений. Каждое планируемое действие становится более взвешенным и ответственным».

Олег Ржевский,
заместитель начальника Управления технической поддержки
Транскапиталбанка, Microsoft MVP

Истории успеха

Netwrix Customer Case Study

Каспийский Трубопроводный Консорциум усилил внутреннюю безопасность ИТ-инфраструктуры с помощью решений Netwrix.

Каспийский Трубопроводный Консорциум контролирует ИТ-инфраструктуру с помощью решений Netwrix

Компания Netwrix завершила проект по оптимизации ИТ-инфраструктуры Каспийского трубопроводного консорциума (КТК) с помощью Netwrix Auditor. Внедрение продукта позволило значительно улучшить видимость и внутреннюю безопасность ИТ-инфраструктуры.

ЗАКАЗЧИК
ЗАО «Каспийский Трубопроводный Консорциум - Р»

САЙТ
cpc.ru

ОТРАСЛЬ
Нефтегазовая

РЕШЕНИЕ
Аудит изменений

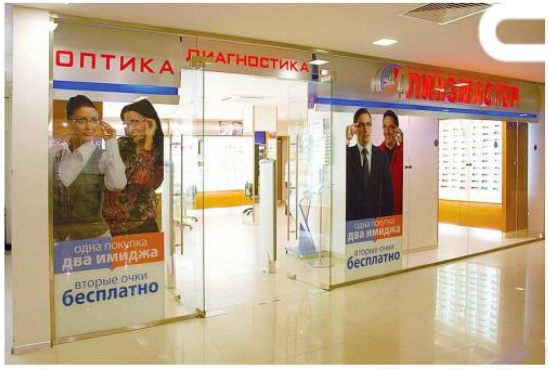
ПРОДУКТ
Netwrix Auditor

ПРОФИЛЬ
Каспийский Трубопроводный Консорциум (КТК) – крупнейший международный нефтетранспортный проект с участием России, Казахстана, а также ведущих мировых добывающих компаний, созданный для строительства и эксплуатации магистрального трубопровода протяженностью более 1,5 тыс. км.

«С первых дней внедрения Netwrix Auditor *были выявлены проблемы различного масштаба, которые были своевременно устранены. Это привело к повышению надежности и защищенности* Active Directory *и сети компании в целом. В дальнейшем мы надеемся получить систему, которая обеспечит нам проактивную защиту от информационных рисков".*

Илья Старков,
ИТ-менеджер КТК.

Netwrix Customer Case Study



Линзмастер контролирует изменения в Active Directory при помощи решений Netwrix

ЗАКАЗЧИК
ООО «Линзмастер»

САЙТ
www.lensmaster.ru

ОТРАСЛЬ
Розничная торговля

РЕШЕНИЕ
Контроль действий пользователей в Active Directory

ПРОДУКТ
Netwrix Auditor – Active Directory

ПРОФИЛЬ
Линзмастер – крупнейшая в России сеть салонов оптики, является частью международной Grandvision Group. Работает в России с 1998 года.

Netwrix объявляет о завершении проекта по внедрению решения Netwrix Auditor - Active Directory для компании Линзмастер. Система позволяет осуществлять контроль изменений в Active Directory и групповых политиках, оперативно реагировать на инциденты ИБ и предотвращать потерю ценной информации.

Компания «Линзмастер» начала свою деятельность на российском рынке в1998 году и на сегодняшний день является крупнейшей оптической сетью в России. «Линзмастер» впервые предложил российскому клиенту полный комплекс услуг – проверка зрения, подбор оправы и линз для очков, изготовление очков, продажа солнцезащитных очков и контактных линз. В 2010 году «Линзмастер» вошел в группу компаний GrandVision, которая является ведущим мировым лидером в оптической рознице. Сейчас в России работает около 100 магазинов сети «Линзмастер»: более 50 магазинов в Москве, более 15 – в Санкт-Петербурге, а также открыты салоны оптики в Казани, Нижнем Новгороде, Екатеринбурге, Ростове-на-Дону, Ярославле, Новосибирске, Самаре, Омске, Краснодаре, Уфе. В штате компании работают более тысячи сотрудников.

Истории успеха

Netwrix Customer Case Study

«Аэроэкспресс» защищает данные Active Directory от нежелательных изменений с помощью ПО Netwrix

Компания «Аэроэкспресс» контролирует изменения в Active Directory с помощью программного обеспечения Netwrix Auditor. Программа позволяет отслеживать любые модификации в системах и приложениях в режиме реального времени, а также оперативно восстанавливать удаленные объекты или настройки.

ЗАКАЗЧИК
ООО «Аэроэкспресс»

САЙТ
www.aeroexpress.ru

ОТРАСЛЬ
Транспорт

РЕШЕНИЕ
Контроль изменений в AD

ПРОДУКТ
Netwrix Auditor

ПРОФИЛЬ ЗАКАЗЧИКА
ООО «Аэроэкспресс» — российская транспортная компания, осуществляющая интермодальные и пригородные пассажирские перевозки в соответствии с лицензией Министерства транспорта РФ. Компания обеспечивает железнодорожное сообщение между центром города и аэропортами в таких городах, как Москва, Владивосток и Казань. «Аэроэкспресс» входит в Международную ассоциацию интермодальных перевозчиков International Air Rail Organization (IARO).

"Использование Netwrix Auditor позволило оперативно разрешать возникающие проблемы. Основное преимущество этого программного обеспечения в том, что оповещения о внесенных изменениях присылаются сразу же, а не спустя сутки или неделю."

Алексей Митюшов,
Зам. директора департамента ИТ по информационной безопасности «Аэроэкспресс»

Netwrix Customer Case Study

Новороссийский Морской Торговый Порт проводит аудит ИТ-инфраструктуры с помощью ПО Netwrix Auditor

Компания Netwrix сообщает о поставке лицензий на ПО Netwrix Auditor в ОАО «Новороссийский морской торговый порт». Программное обеспечение отслеживает изменения в основных системах и приложениях, предотвращая сбои в работе ИТ-инфраструктуры и потерю данных.

ЗАКАЗЧИК
ОАО «НОВОРОССИЙСКИЙ МОРСКОЙ ТОРГОВЫЙ ПОРТ» (ОАО «НМТП»)

САЙТ
www.nmtp.info

ОТРАСЛЬ
Транспорт

РЕШЕНИЕ
Контроль изменений

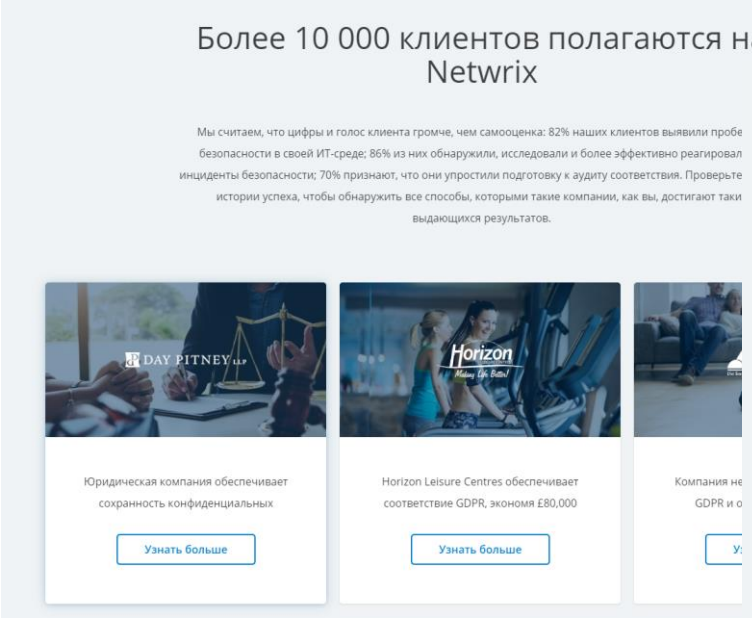
ПРОДУКТ
Netwrix Auditor

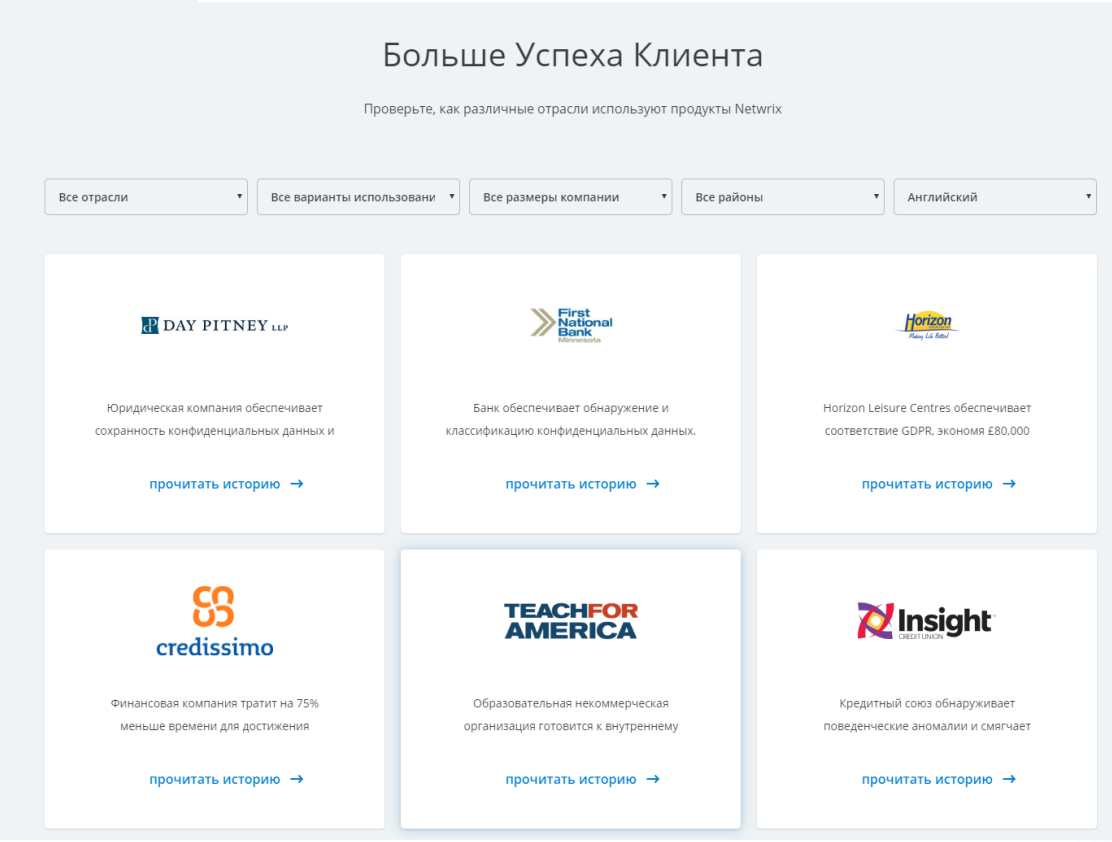
ПРОФИЛЬ ЗАКАЗЧИКА

Группа НМТП – ведущий стивидорный оператор в России, занимает третье место среди европейских портов по объему грузооборота. Группа НМТП объединяет ОАО "НМТП", ООО "Приморский торговый порт", ОАО "Новороссийский зерновой терминал", ОАО "Новороссийский судоремонтный завод", ОАО "Флот НМТП", ОАО "Новорослесэкспорт", ОАО "ИПП", ООО "Балтийская стивидорная компания" и ЗАО "СФП".

Портал историй успеха Netwrix

https://www.netwrix.com/customer_case_studies.html





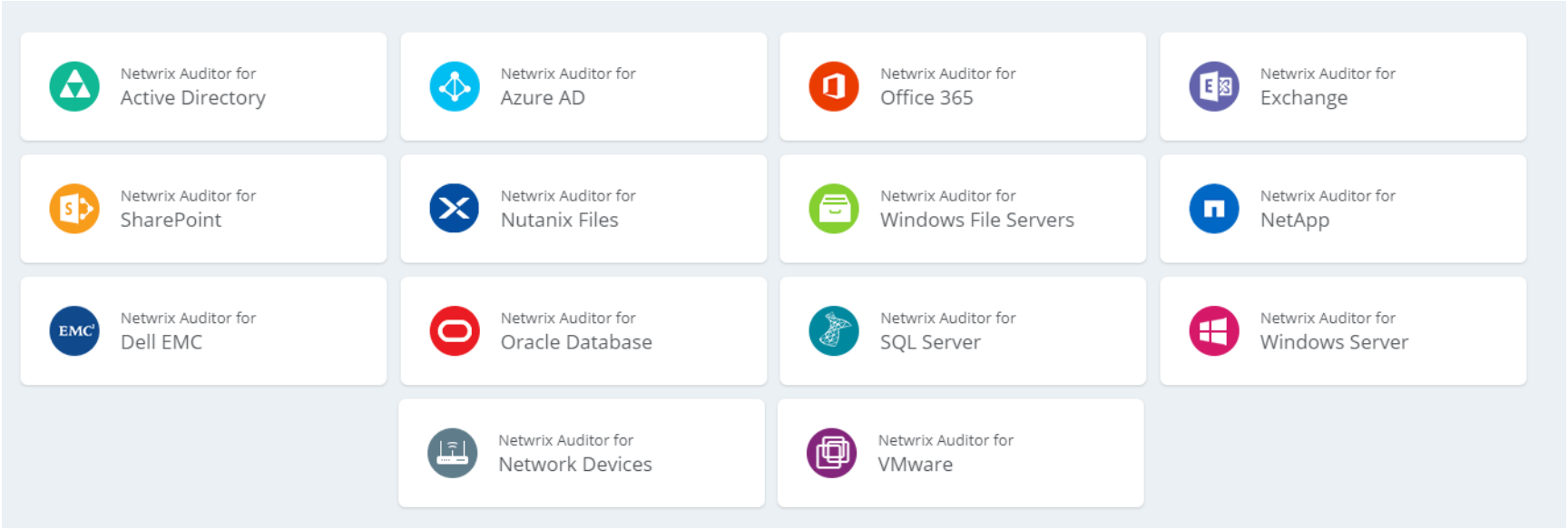
Техническая часть

1. Как проводить оценку рисков, находить и ликвидировать слабые места в защите серверов под управлением Windows ;
2. Как выявить и защитить конфиденциальные данные;
3. Как настроить уведомления так, чтобы не пропустить важные ИБ-инциденты и избавиться от лишних оповещений;
4. Как защитить серверы под управлением Windows от внутренних и внешних угроз.
5. Получите информацию о защите данных с помощью Netwrix Auditor.
6. Получите информацию о единой платформе для мониторинга всех событий в системах хранения данных и ИТ-инфраструктуре.
7. Узнайте о возможности анализа конфиденциальных данных, каким рискам они подвергаются, какие действия угрожают их безопасности.
8. Узнайте о возможности снизить риски и вовремя обнаружить угрозы, предотвратить утечку данных и обеспечить соответствие политик информационной безопасности требованиям законодательства.
9. Улучшите защиту конфиденциальной информации за счет ограничений прав доступа и снижения рисков ИБ.
10. Получите информацию о выявлении и оценке инцидентов благодаря отчетам об аномальной активности и оценке рисков.
11. Узнайте о возможности анализа конфиденциальных данных с помощью Data Discovery and Classification, каким рискам они подвергаются, какие действия угрожают их безопасности.

Техническая часть

- Ищете решение, которое обеспечит единообразное и последовательное представление такой информации?
- Netwrix Auditor хранит консолидированные данные аудита различных ИТ-систем,

в том числе Active Directory, Windows Server, баз данных Oracle и сетевых устройств.



Сценарии решений Netwrix Auditor

Оценивайте риски и устраняйте уязвимости

Выявляйте проблемы ИБ, такие как права доступа, предоставленные без использования групповых политик безопасности, или неактивные учетные записи пользователей, и устраняйте их, чтобы снизить поверхность атаки.

Автоматизируйте поиск и классификацию данных

Защитите критически важную информацию: выявляйте конфиденциальные данные в хранилищах и регулярно проверяйте, кто имеет к ним доступ и как они используются.

Экономьте время благодаря отчетам об изменениях, правах доступа и конфигурации систем

Быстро находите информацию, нужную руководителям компании и аудиторам. Больше не нужно мучаться со скриптами, логами и таблицами.

Своевременно узнавайте о потенциальных угрозах

Оперативно получайте уведомления о любых подозрительных действиях в ИТ-инфраструктуре, чтобы принять меры для предотвращения утечки данных, сбоев в работе или штрафов за несоблюдение нормативных требований.

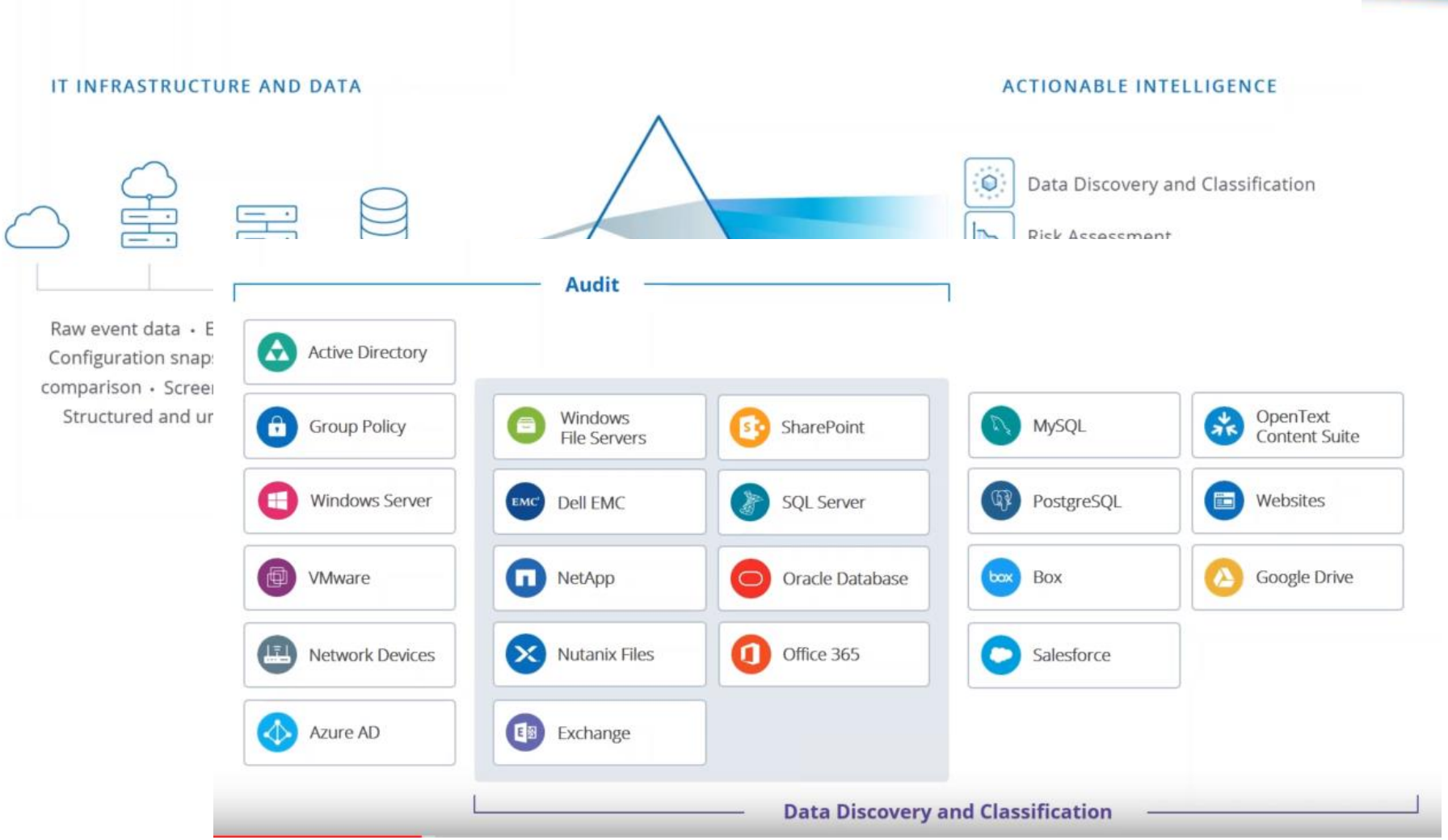
Эффективнее выявляйте сложные угрозы

Обнаруживайте внутренних злоумышленников и взломанные учетные записи с помощью единой системы мониторинга подозрительной активности пользователей и системы расчёта уровня риска для каждой учетной записи.

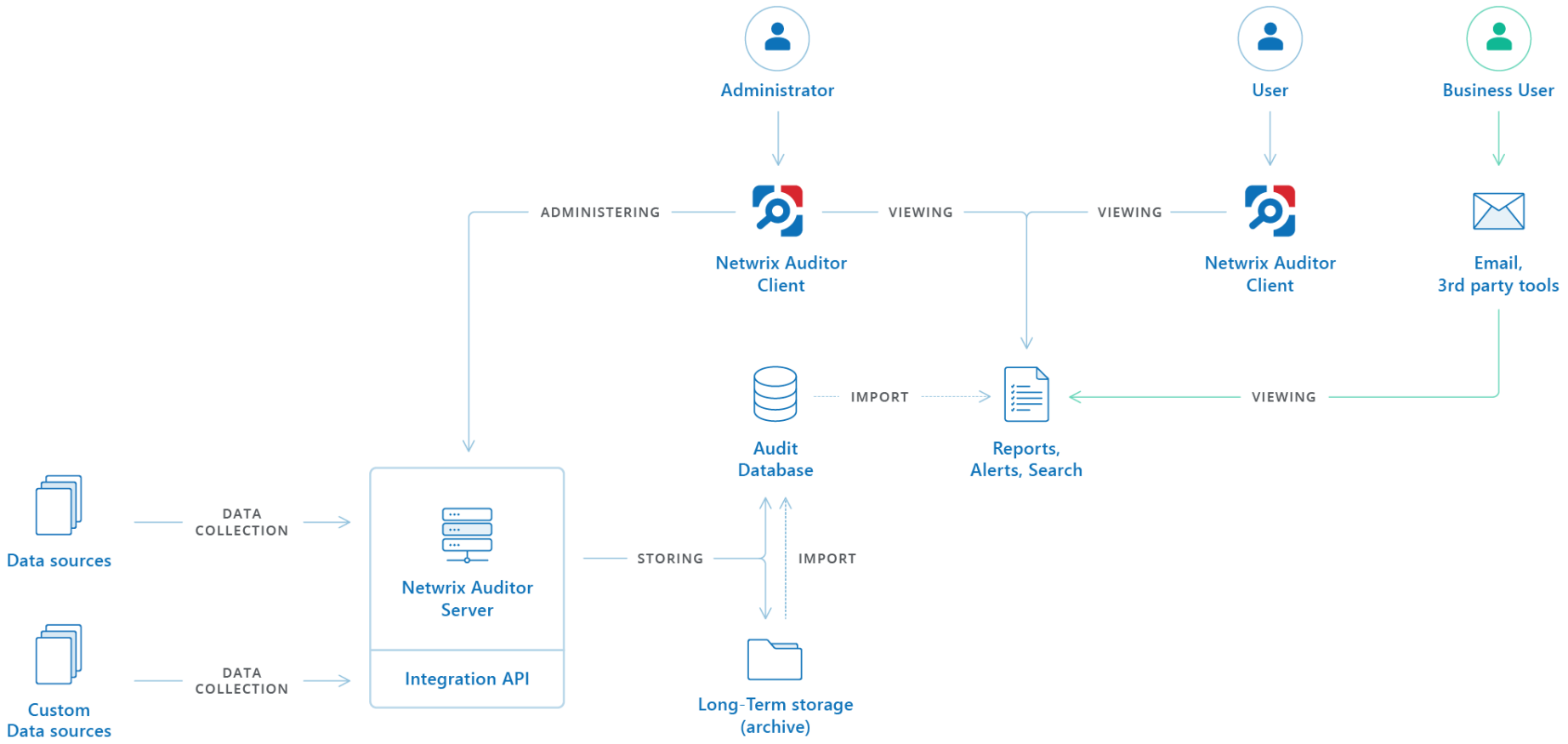
Находите ответы с помощью поиска, как в Google

Всего за несколько кликов вы найдете нужные блоки информации, которые позволят выяснить причину ИБ-инцидента, решить проблему пользователя или ответить на неожиданный вопрос аудиторов.

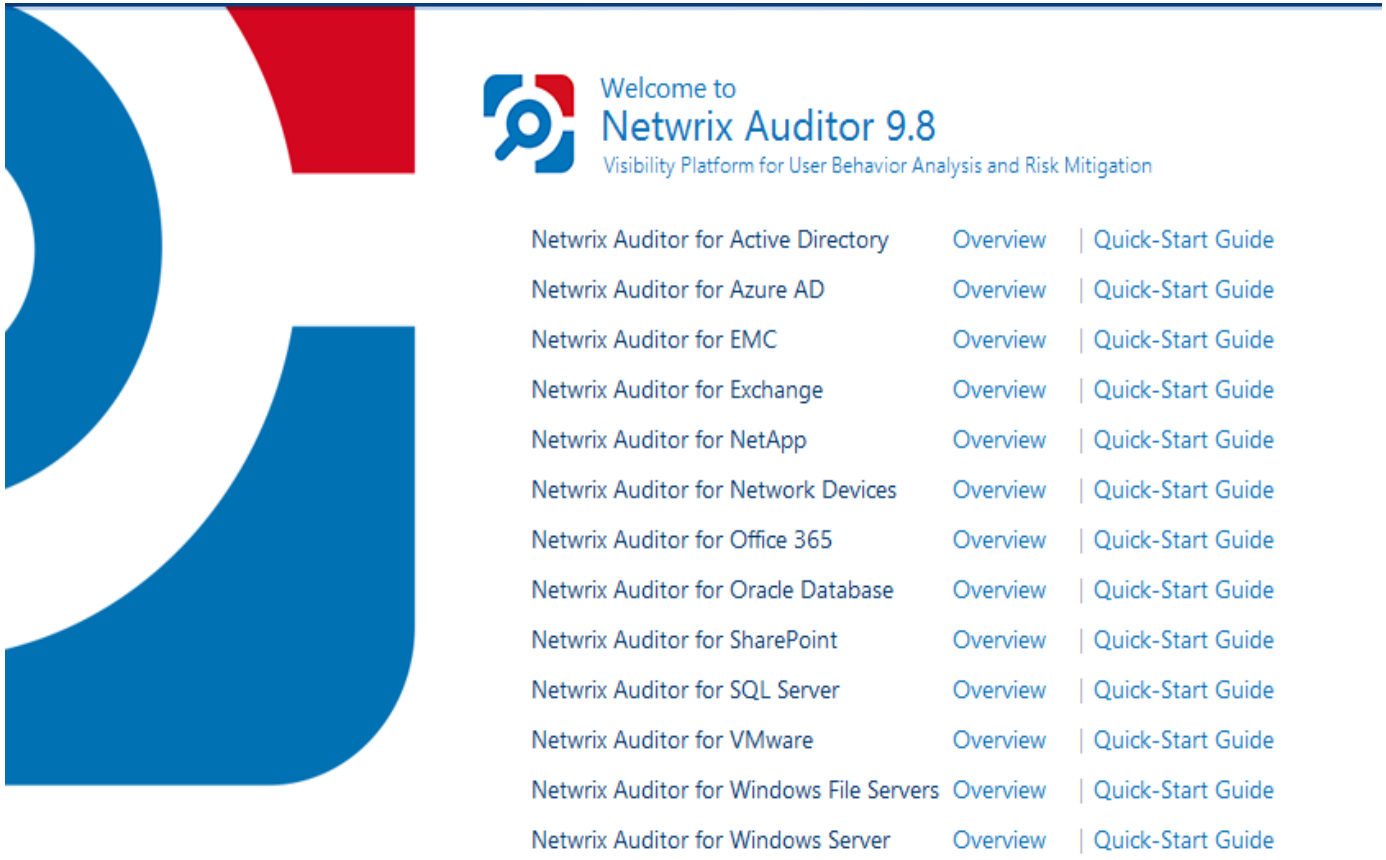
Общая идеология решения



Архитектура Netwrix Auditor



Дистрибутив в разных форматах



Дистрибутив доступен на сайте в виде

- файла

- виртуальной машины

- для развертывания в облаке Azure или AWS

Релиз 9.9 (декабрь 2019)

Возможности версии 9.9

Само-аудит

Менеджер учетных записей

Новые дашборды

Новости о продукте

Поддержка протокола TCP для аудита сетевых устройств

Поддержка Oracle 19C

Новые отчеты «Все изменения» без SSRS

Релиз 9.9 (новая функциональность)

Новая функциональность

Несанкционированные попытки входа в AD FS

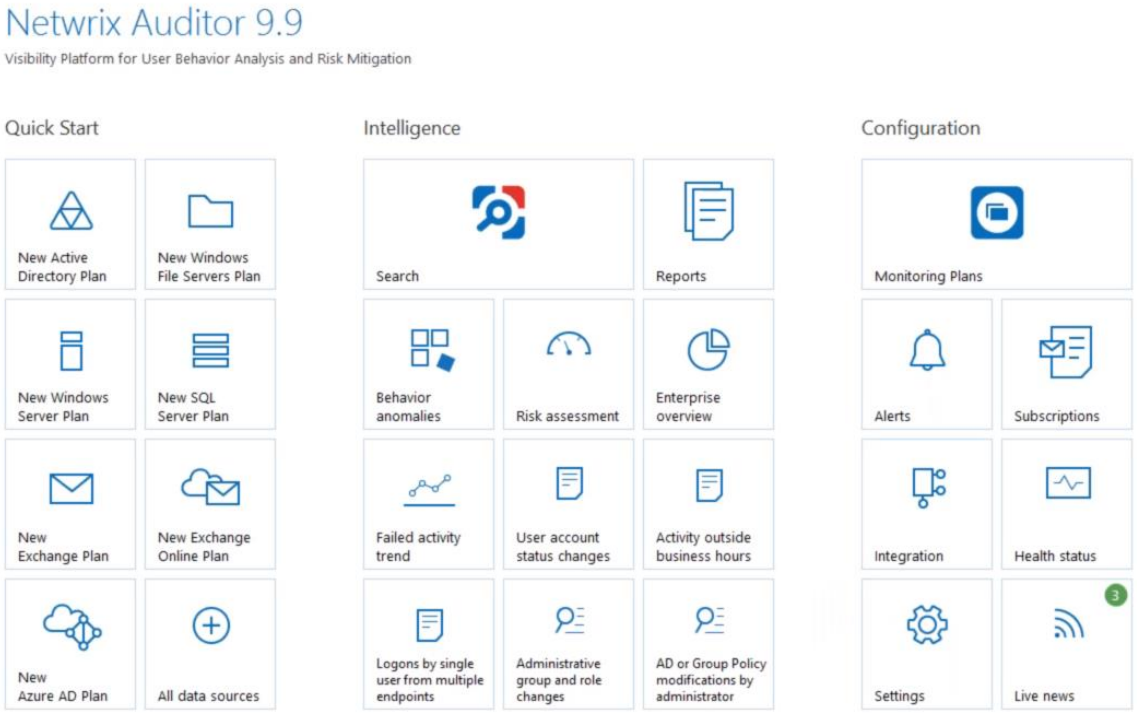
Несанкционированные попытки входа в VmWare ESXi и VCenter

Права доступа к SharePoint Online и One Drive for Business

Права доступа к почтовым ящикам Exchange Online

Аддон для CyberArk Privileged Access Security

Функции администратора в консоли



- Управление заданиями
- Добавление целевых систем
- Авт. включение аудита
- Назначение ролей
- Настройки продукта
- Управление лицензиями
- Управление адд-онами

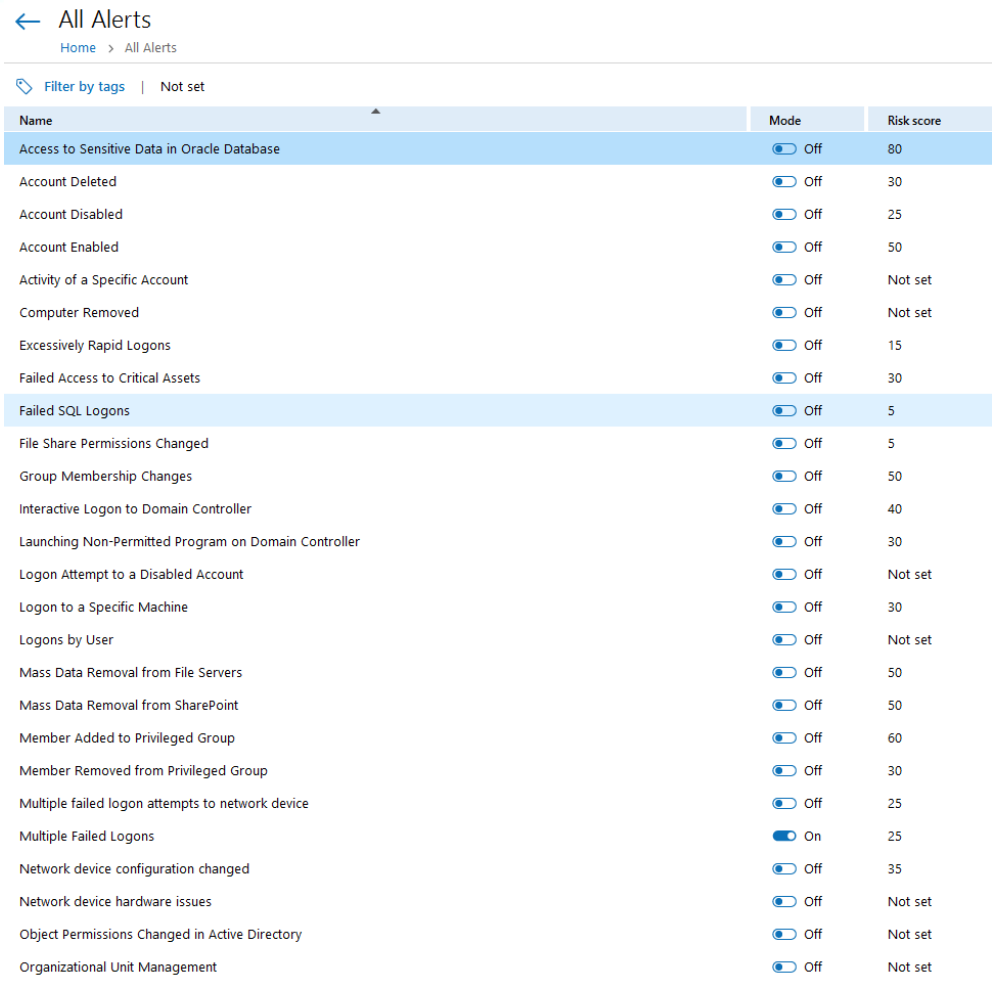
Ключевые вопросы аудита

Платформа	Типовые вопросы аудита
Active Directory	• Кто добавил пользователя в группу? • Кто успешно вошел в систему / не смог войти? • Кто делегировал подразделению права управления?
VMware	• Кто создал новую виртуальную машину? • Кто изменил параметры пула ресурсов?
MS Exchange	• Кто удалил почтовый ящик? • Кто получил доступ к почтовому ящику другого пользователя? • Кто изменил настройки службы Information Store?
SQL Server	• Кто изменил структуру таблицы в базе данных SQL? • Кто удалил базу данных SQL? • Кто добавил новый логин?
File Server	• Кто изменил права доступа к файлам NetApp Filer? • Кто просматривал важные файлы на файловых серверах? • Кто удалил файлы с файлового сервера?
Group Policy	• Кто отключил усиленную политику паролей? • Кто отключил объект GPO от подразделения? • Кто настроил новую политику установки ПО?
Server Configuration	• Кто устанавливал ПО и какое именно? • Кто внес изменения в системный реестр? • Кто изменил настройки конфигурации компьютера?
SharePoint	• Какие веб-приложения создавались/менялись/удалялись? • Какие серверы были добавлены к ферме либо удалены? • Как изменились настройки входящих/исходящих сообщений электронной почты?
SCVMM Environments	• Какие произведены изменения в настройках виртуальных машин? • Какие виртуальные машины были добавлены/удалены?
Сетевые устройства	• Какое новое устройство добавлено в сеть? • Кто изменил настройки сетевого монитора? (*) • Кто изменил таблицу маршрутизации на роутере? (*) • Какой учетной записи предоставлены привилегии администратора сетевого монитора? (*) • Какое устройство было удалено из сети?

Netwrix Auditor

Аудит и отчеты о соответствии стандартам ИБ

Интеллектуальные возможности



Name	Mode	Risk score
Access to Sensitive Data in Oracle Database	Off	80
Account Deleted	Off	30
Account Disabled	Off	25
Account Enabled	Off	50
Activity of a Specific Account	Off	Not set
Computer Removed	Off	Not set
Excessively Rapid Logons	Off	15
Failed Access to Critical Assets	Off	30
Failed SQL Logons	Off	5
File Share Permissions Changed	Off	5
Group Membership Changes	Off	50
Interactive Logon to Domain Controller	Off	40
Launching Non-Permitted Program on Domain Controller	Off	30
Logon Attempt to a Disabled Account	Off	Not set
Logon to a Specific Machine	Off	30
Logons by User	Off	Not set
Mass Data Removal from File Servers	Off	50
Mass Data Removal from SharePoint	Off	50
Member Added to Privileged Group	Off	60
Member Removed from Privileged Group	Off	30
Multiple failed logon attempts to network device	Off	25
Multiple Failed Logons	On	25
Network device configuration changed	Off	35
Network device hardware issues	Off	Not set
Object Permissions Changed in Active Directory	Off	Not set
Organizational Unit Management	Off	Not set

Расследование инцидентов

- Интерактивный поиск
- 300 готовых отчетов
- Пользовательские отчеты
- Видеозапись действий

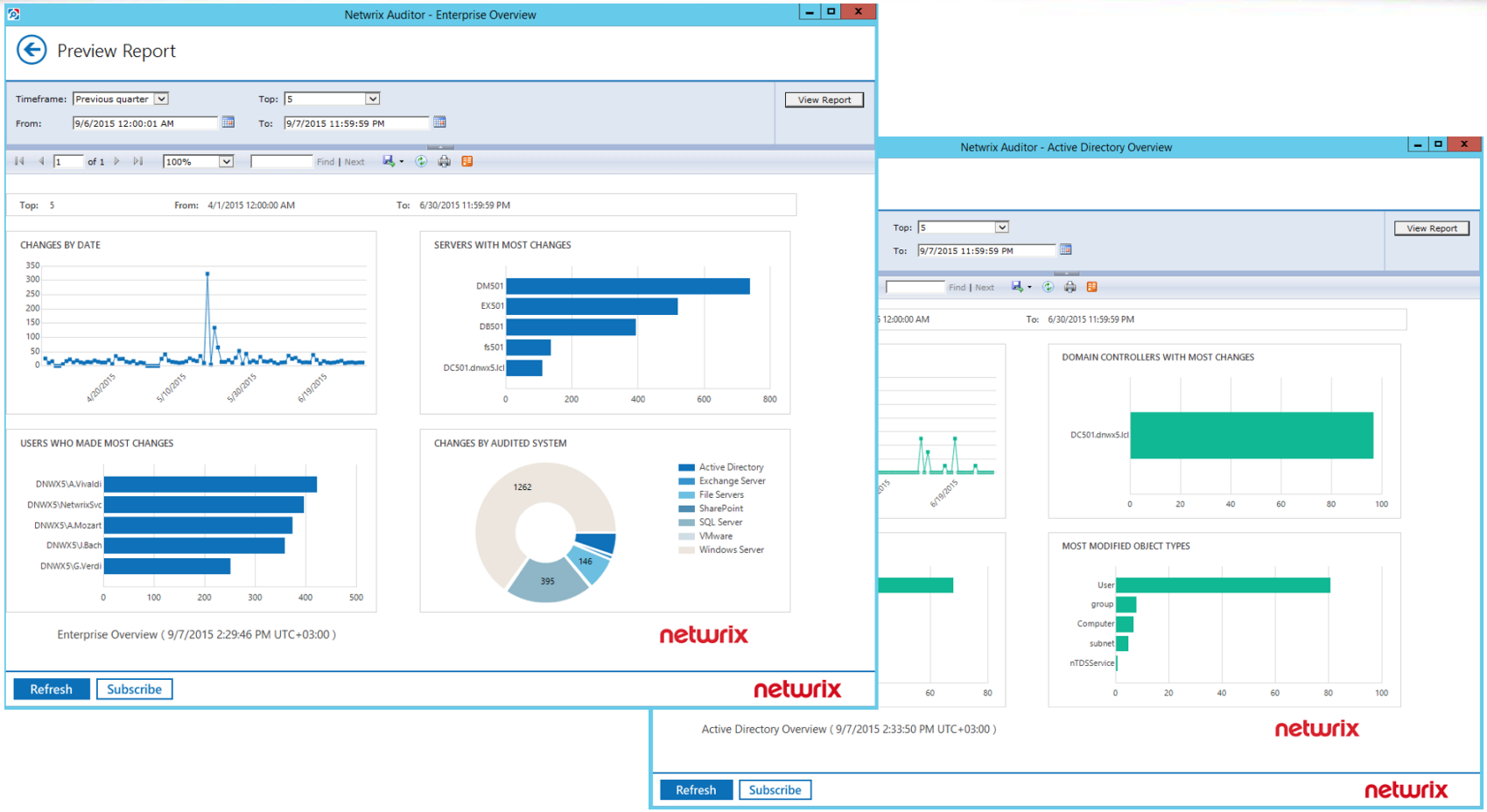
- Выявление аномалий

- Оценка рисков

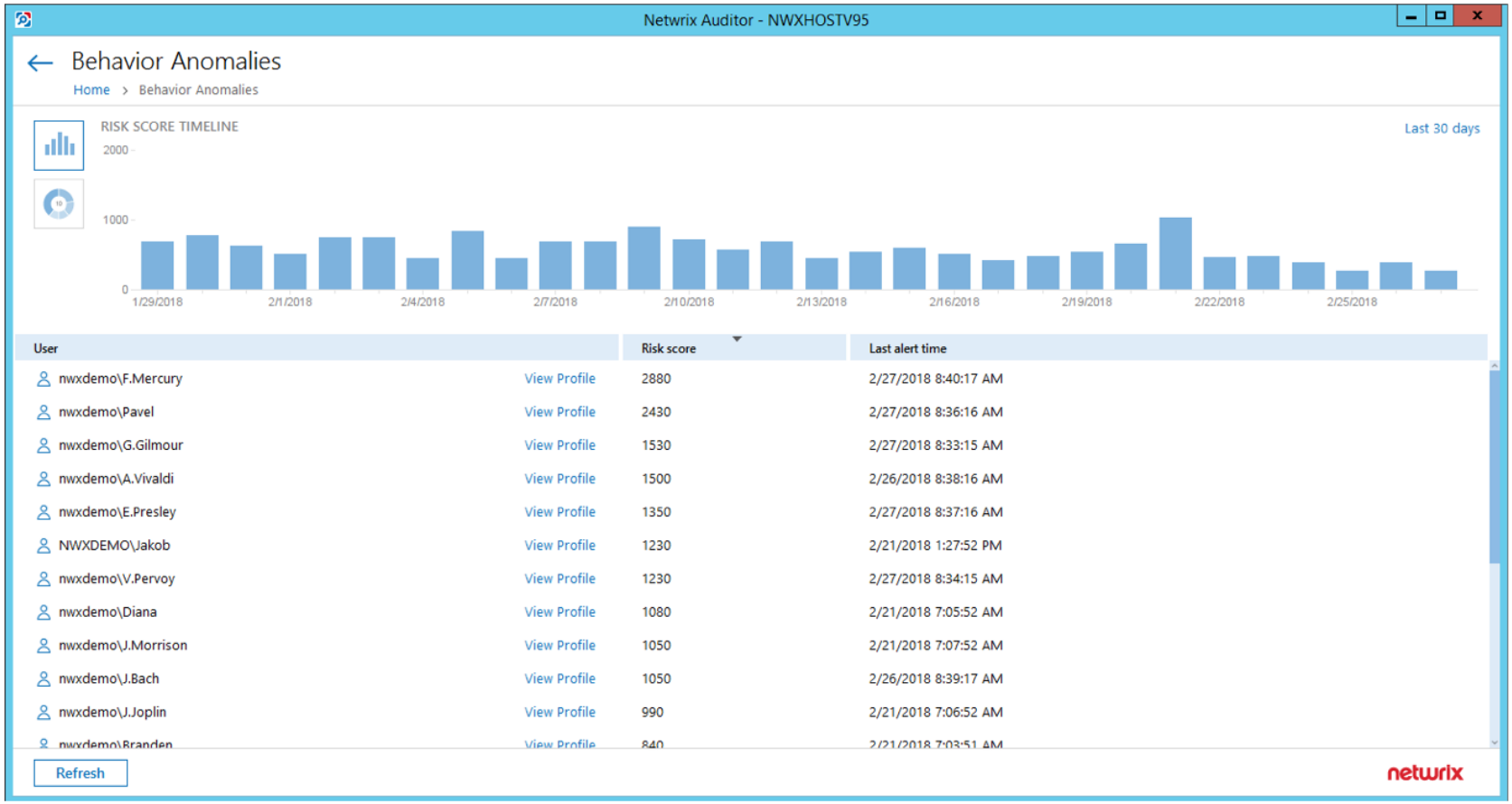
- Классификатор данных

- Пороговые значения для оповещений

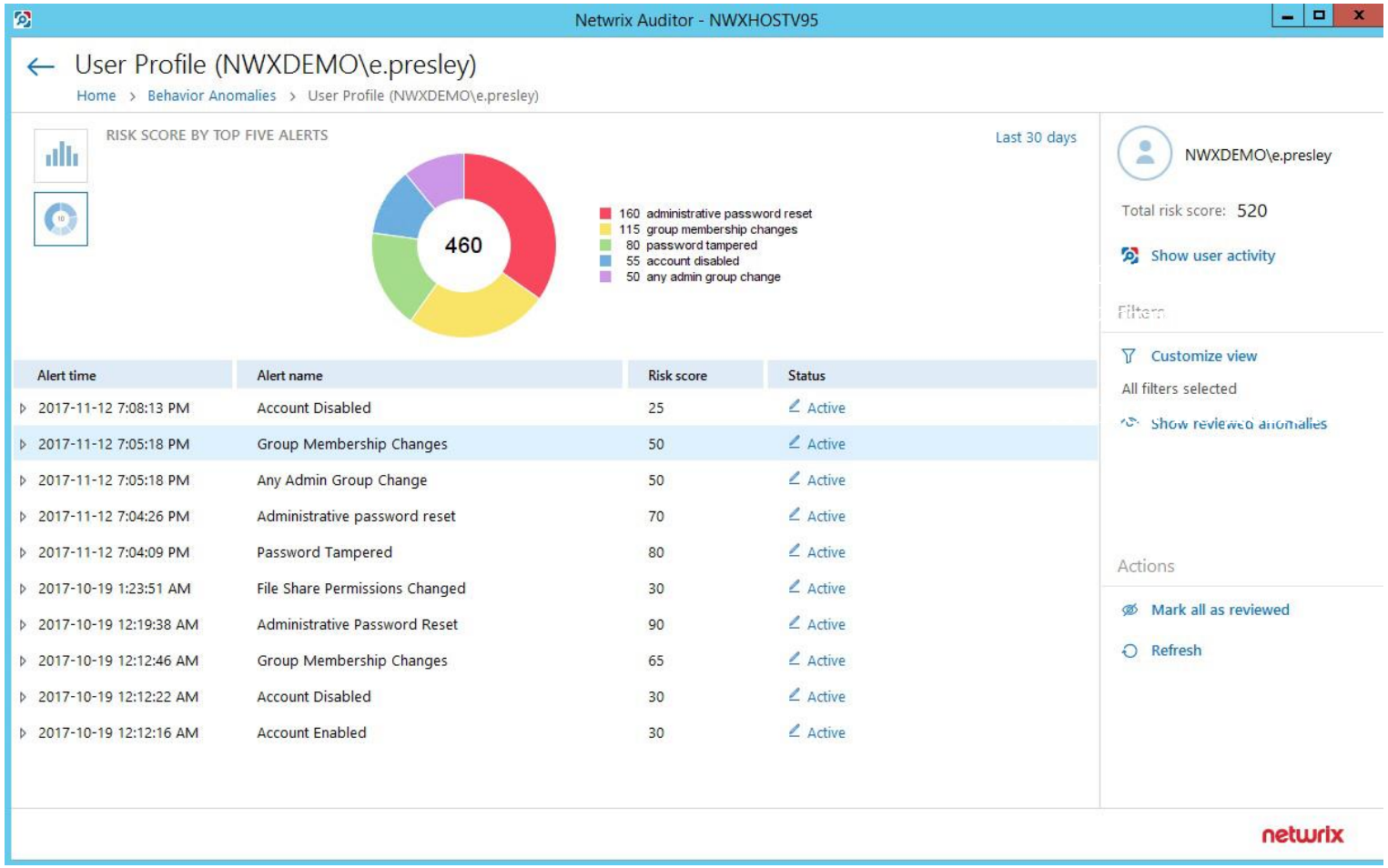
Обзор изменений во всех системах



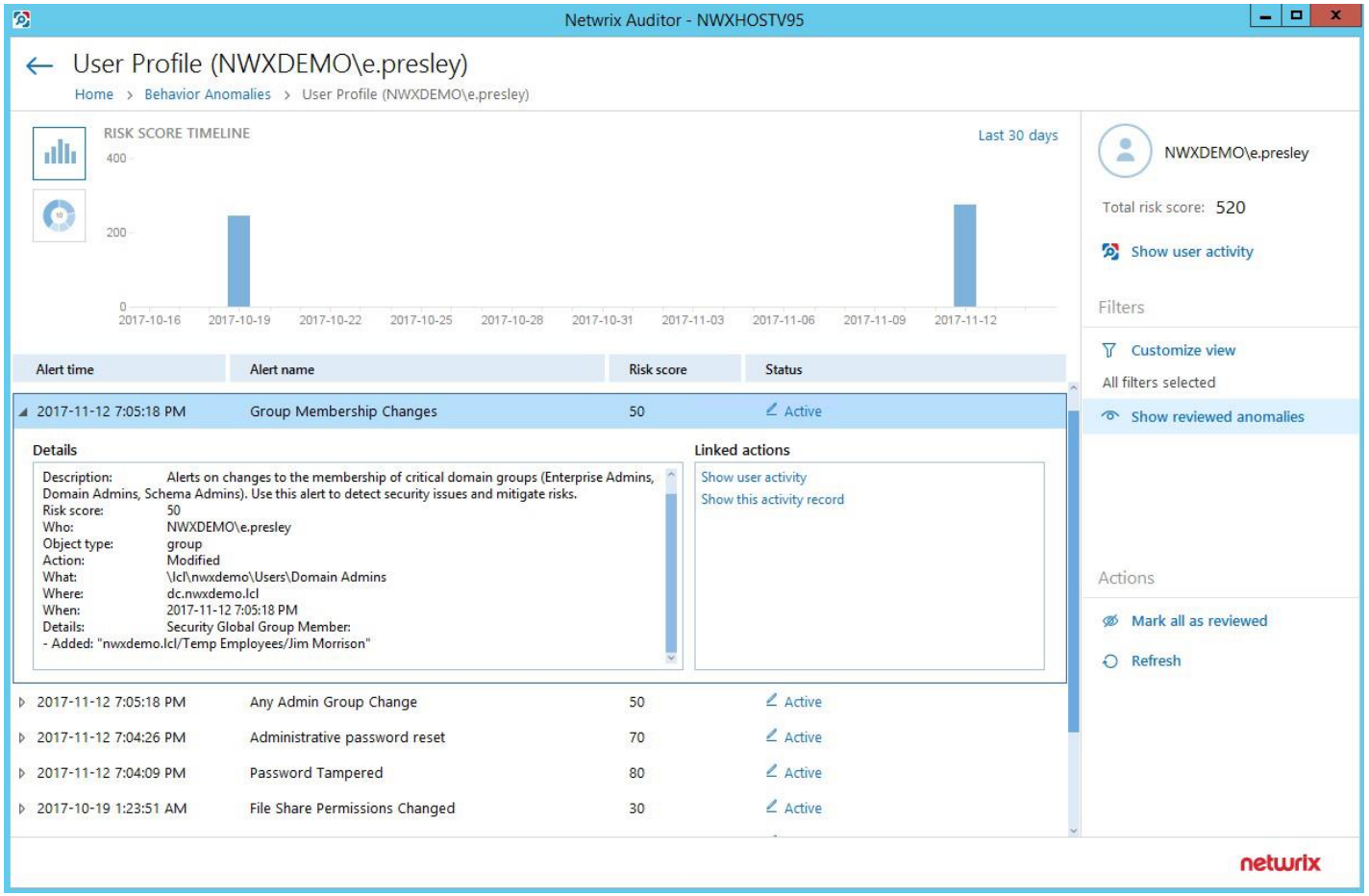
Аномальное поведение на шкале времени



Профиль подозреваемого



Детали по каждому действию



Действия пользователя во всех системах

Netwrix Auditor Tuesday, April 22, 2014 4:39 PM

All Changes by User

Shows all changes across the entire IT infrastructure grouped by the users who made the changes.

Filter	Value

Who Changed: CITY\Megan

Audited System: Active Directory

Action	Object Type	What Changed	Where Changed	When Changed
Modified	**User**	\local\city\People\Bill	chicago.city.local	3/20/2014 8:35:55 PM
Principal Name set to "Bill@city.local"				
Removed	**User**	\local\city\People\Sophia	chicago.city.local	3/20/2014 8:36:04 PM

Audited System: Windows Servers

Action	Object Type	What Changed	Where Changed	When Changed
Removed	**Registry Key**	Registry\HKEY_LOCAL_MACHINE\software\Microsoft\Windows\CurrentVersion\Installer\InProgress	2k8	10/23/2013 6:29:14 PM
(REG_SZ): "C:\Windows\Installer\591ac9.ipi"				
Ownership: "Owner: NT AUTHORITY\SYSTEM"				

Audited System: VMware

Action	Object Type	What Changed	Where Changed	When Changed
Removed	**VirtualMachine**	\ha-folder-root\ha-datacenter\vm\kn	https://10.0.4.48:443	10/25/2013 6:38:42 PM

Audited System: SQL Servers

Action	Object Type	What Changed	Where Changed	When Changed
Added	**Database**	Databases\fj	w2012dc1	10/24/2013 9:19:28 PM

Netwrix Auditor Thursday, April 10, 2014 7:01 AM

All Changes by Audited System

Shows all changes across the entire IT infrastructure grouped by the audited system.

Filter	Value

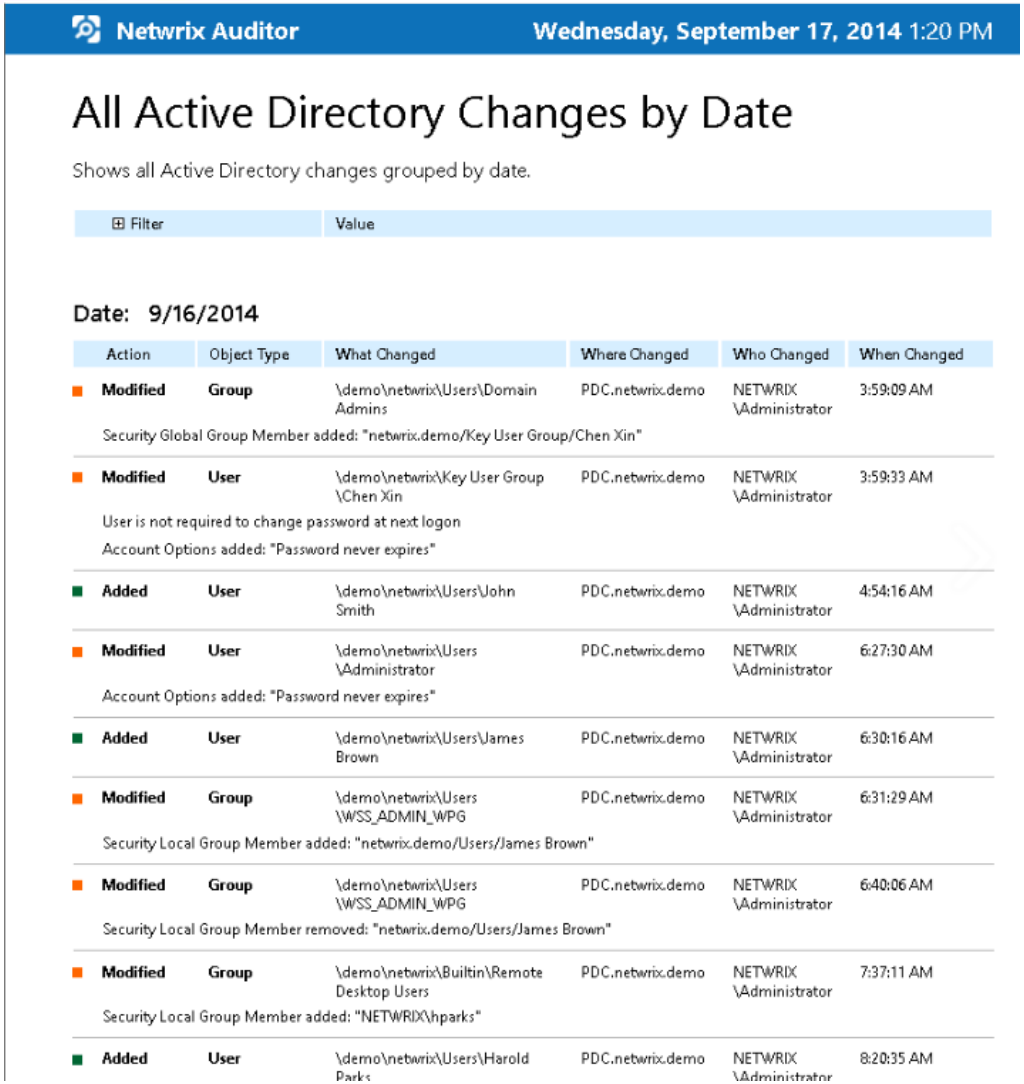
Audited System: Active Directory

Action	Object Type	What Changed	Where Changed	Who Changed	When Changed
Added	**User**	\local\corp\Users\John Smith	rootdc1.corp.local	CORP\administrator	2/26/2014 5:17:56 AM
Added	**User**	\local\corp\Users\Brad Davis	rootdc1.corp.local	CORP\administrator	3/5/2014 4:55:26 AM
Added	**User**	\local\corp\Users\Greg Taylor	rootdc1.corp.local	CORP\administrator	3/6/2014 1:18:06 AM
Added	**User**	\local\corp\Users\Bob Brown	rootdc1.corp.local	CORP\administrator	3/6/2014 1:19:29 AM
Modified	**Group**	\local\corp\Users\Domain Admins	rootdc1.corp.local	CORP\administrator	3/19/2014 7:42:06 AM
Security Global Group Member added: "corp.local/Users/John Smith"					
Added	**User**	\local\corp\Users\Thomas Moore	rootdc1.corp.local	CORP\administrator	3/20/2014 1:50:06 AM
Added	**Group**	\local\corp\Users\Accountants	rootdc1.corp.local	CORP\administrator	3/20/2014 1:51:44 AM
Group Type "Security Domain Local Group"					
Members "\local\corp\Users\Thomas Moore"					
Added	**User**	\local\corp\Users\Anna Thompson	rootdc1.corp.local	CORP\administrator	3/20/2014 1:52:22 AM
Modified	**Group**	\local\corp\Users\Accountants	rootdc1.corp.local	CORP\administrator	3/20/2014 1:52:56 AM
Security Local Group Member added: "corp.local/Users/Anna Thompson"					
Added	**User**	\local\corp\Users\Sheila Hartford	rootdc1.corp.local	CORP\administrator	3/20/2014 1:53:57 AM

Netwrix Auditor for Active Directory

групповые политики, возврат изменений, доп. инструменты

Пример отчета: изменения в AD за день



Netwrix Auditor — Wednesday, September 17, 2014 1:20 PM

All Active Directory Changes by Date

Shows all Active Directory changes grouped by date.

⊞ Filter	Value

Date: 9/16/2014

Action	Object Type	What Changed	Where Changed	Who Changed	When Changed
Modified	**Group**	\demo\netwrix\Users\Domain Admins	PDC.netwrix.demo	NETWRIX \Administrator	3:59:09 AM
Security Global Group Member added: "netwrix.demo/Key User Group/Chen Xin"					
Modified	**User**	\demo\netwrix\Key User Group \Chen Xin	PDC.netwrix.demo	NETWRIX \Administrator	3:59:33 AM
User is not required to change password at next logon					
Account Options added: "Password never expires"					
Added	**User**	\demo\netwrix\Users\John Smith	PDC.netwrix.demo	NETWRIX \Administrator	4:54:16 AM
Modified	**User**	\demo\netwrix\Users \Administrator	PDC.netwrix.demo	NETWRIX \Administrator	6:27:30 AM
Account Options added: "Password never expires"					
Added	**User**	\demo\netwrix\Users\James Brown	PDC.netwrix.demo	NETWRIX \Administrator	6:30:16 AM
Modified	**Group**	\demo\netwrix\Users \WSS_ADMIN_WPG	PDC.netwrix.demo	NETWRIX \Administrator	6:31:29 AM
Security Local Group Member added: "netwrix.demo/Users/James Brown"					
Modified	**Group**	\demo\netwrix\Users \WSS_ADMIN_WPG	PDC.netwrix.demo	NETWRIX \Administrator	6:40:06 AM
Security Local Group Member removed: "netwrix.demo/Users/James Brown"					
Modified	**Group**	\demo\netwrix\Builtin\Remote Desktop Users	PDC.netwrix.demo	NETWRIX \Administrator	7:37:11 AM
Security Local Group Member added: "NETWRIX\hparks"					
Added	**User**	\demo\netwrix\Users\Harold Parks	PDC.netwrix.demo	NETWRIX \Administrator	8:20:35 AM

Пример отчета: изменения в группах

Netwrix Auditor — Wednesday, February 24, 2016 2:55 PM

Security Groups Changes

Shows changes to security groups (permissions, membership, descriptions, etc.), and affected parent groups.

Filter	Value

Who: ENTERPRISE\J.Carter

Action	What	Scope	When
Modified	\com\enterprise\Managers\Managers	Security Global Group	1/11/2016 4:17:22 AM

Where: DC1.enterprise.com

Security Global Group Member:

- Added: "enterprise.com/Managers/Harry Malicious"

Who: ENTERPRISE\T.Simpson

Action	What	Scope	When
Modified	\com\enterprise\Users\Domain Admins	Security Global Group	1/13/2016 12:43:00 PM

Where: DC1.enterprise.com

Security Global Group Member:

- Added: "enterprise.com/Users/Peter Anderson"

Action	What	Scope	When
Modified	\com\enterprise\Users\ChangeAuditor Administrators - DELLCA	Security Domain Local Group	1/13/2016 12:43:24 PM

Where: DC1.enterprise.com

Security Local Group Member:

- Added: "enterprise.com/Users/Peter Anderson"

Выявление неактивных пользователей

Track Inactive Users

Netwrix Auditor audits and automates the management of inactive user accounts.

- [x] Enable inactive user tracking

Consider user inactive after 1 days of inactivity

Actions

- [x] Notify manager after 40 days of inactivity
- [x] Set random password after 55 days of inactivity
- [x] Disable account after 80 days of inactivity
- [x] Move to a specific OU after 120 days of inactivity
  - OU name: NETWRIX/Users ...
- [ ] Delete accounts after 360 days of inactivity

Scope

- [ ] Filter by account name: *
- [ ] Filter by organizational unit — Select OUs...
- [x] Process user accounts
- [ ] Process computer accounts
- [ ] Delete account with all its subnodes (Windows 2008 or above)
- [ ] Notify managers only once

Reporting

Send reports to: Administrator@netwrix.demo — Verify

Edit e-mail template: Edit...

- [ ] Attach report as a CSV file

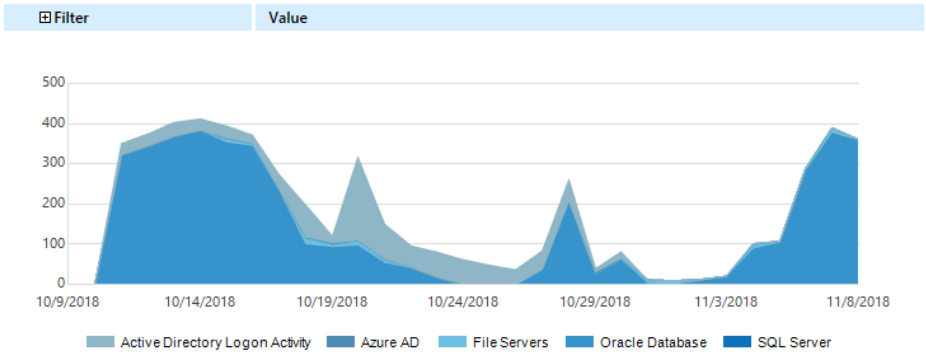
Netwrix Auditor Alert

Member Added to Privileged Group

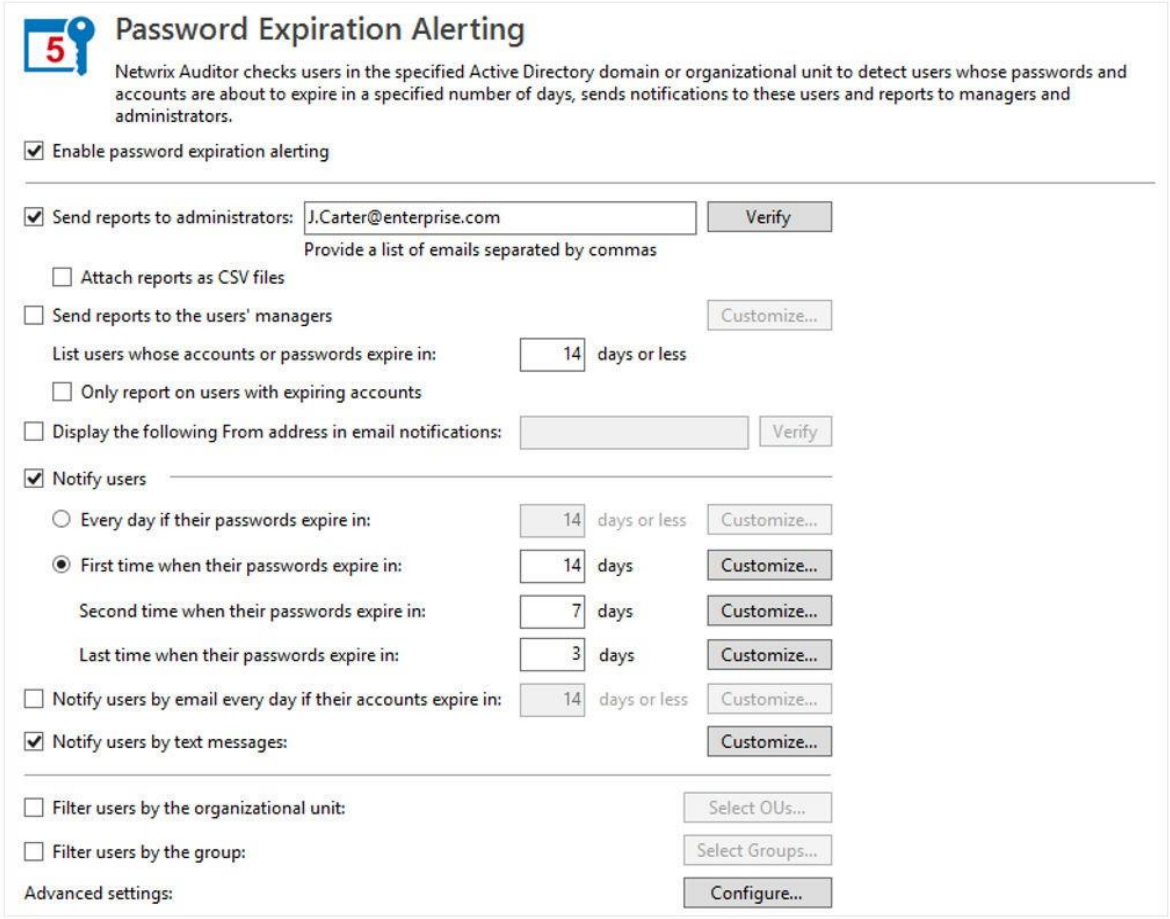
Alerts when a user is added to one of the critical domain groups (Enterprise Admins, Domain Admins, Schema Admins).

Who:	NWXDEMO\a.tkach
Action:	Modified
Object type:	group
What:	\lcl\nwxdemo\Users\Domain Admins
When:	7/18/2018 6:05:25 PM
Where:	dc.nwxdemo.lcl
Workstation:	172.17.6.59
Data source:	Active Directory
Monitoring plan:	Active Directory
Item:	nwxdemo.lcl (Domain)
RID:	20180718151600271E41C521C9BE24044B401F7471260D2AC
Details:	Security Global Group Member: - Added: "nwxdemo.lcl/Temp Employees/Elvis Presley"

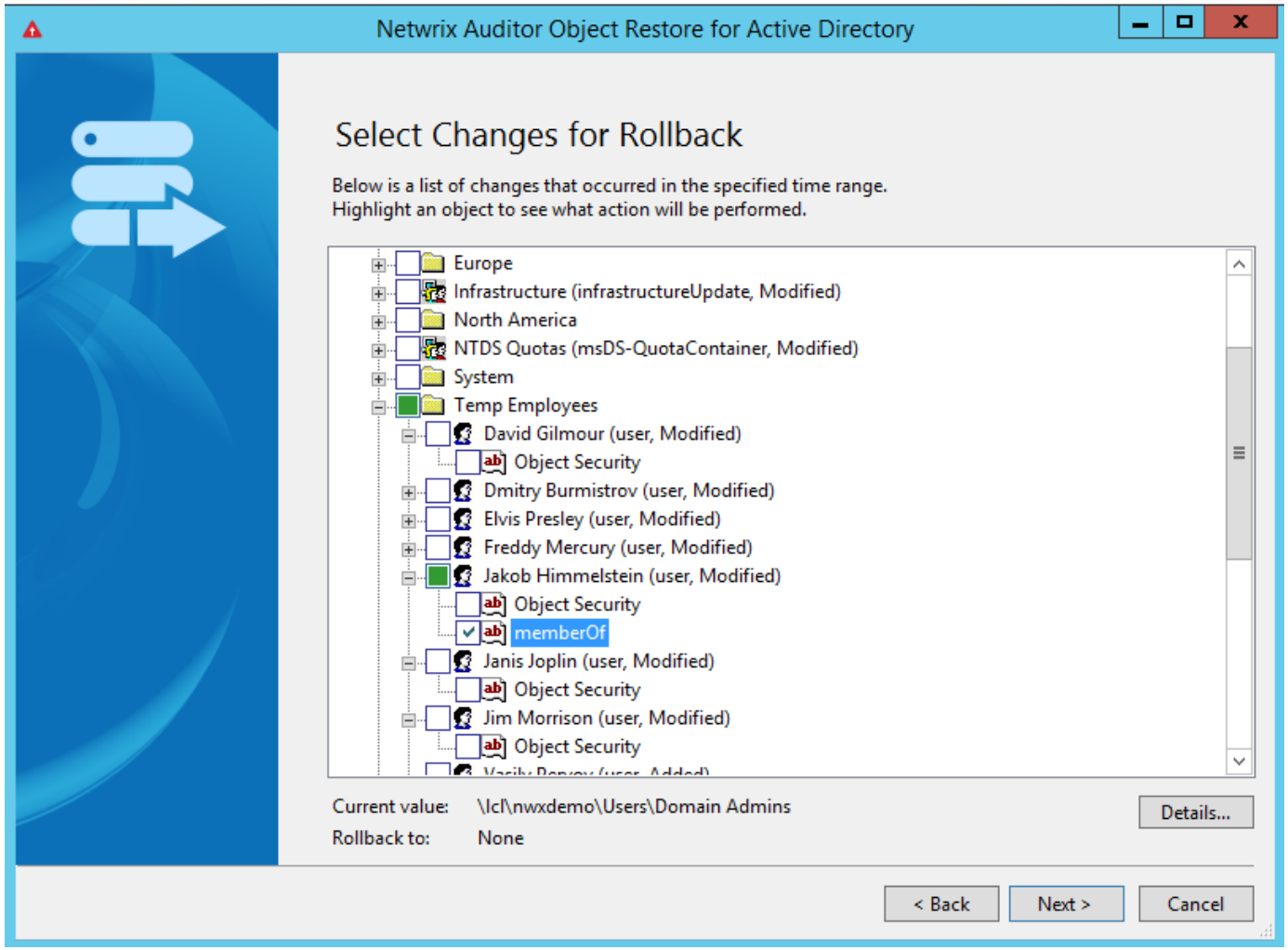
Failed Activity Trend



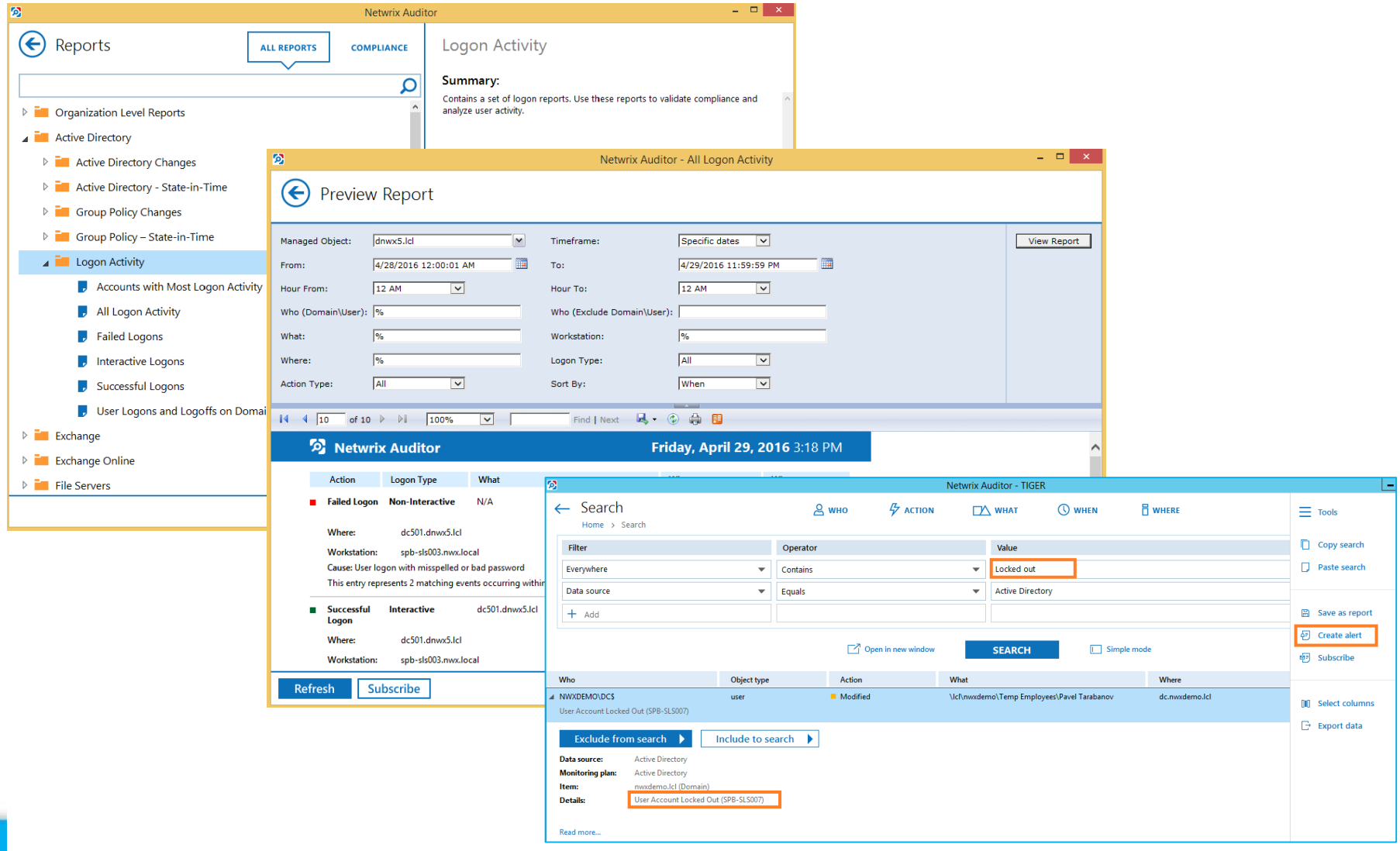
Напоминание об истекающих паролях



Возврат нежелательных изменений в AD



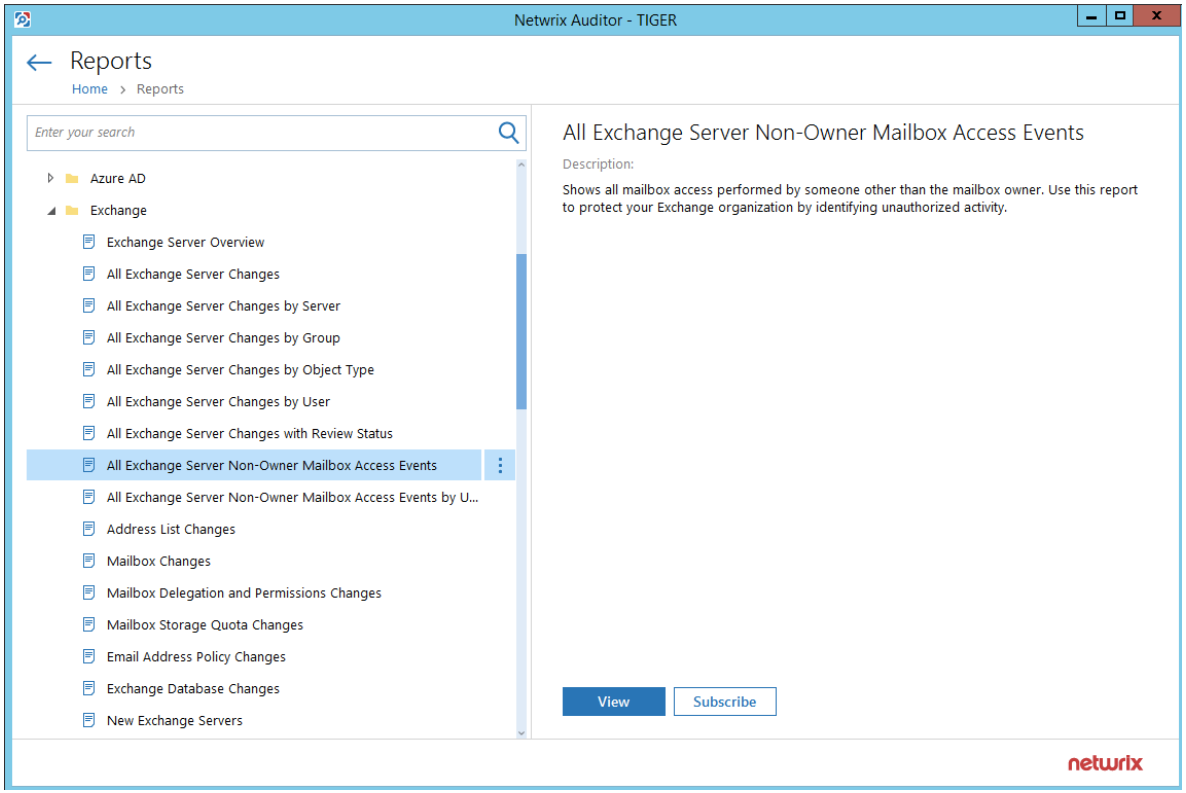
Мониторинг входов и заблокированных учеток



Netwrix Auditor for Exchange

мониторинг изменений на сервере и в общих почтовых ящиках

Контроль изменений в Exchange



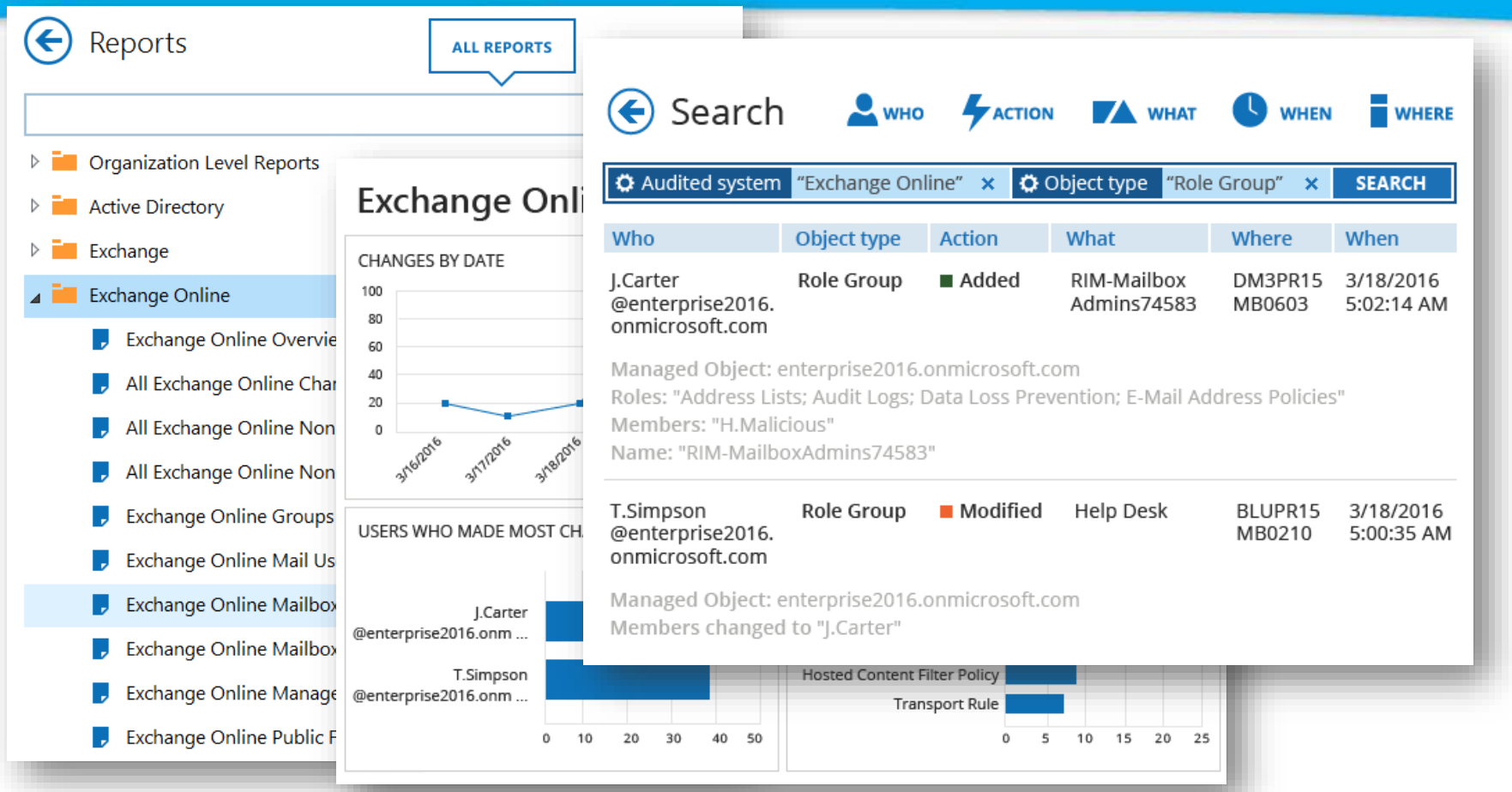
- Настройки Exchange

- Изменения в почтовых ящиках (квоты и пр.)

- Изменения прав

- Подробно: действия в общих почтовых ящиках

Поиск и отчеты об изменениях в Exchange Online

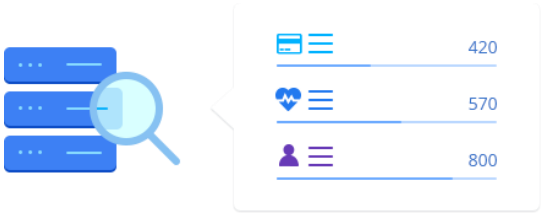


Классификатор данных

Вопросы классификации данных

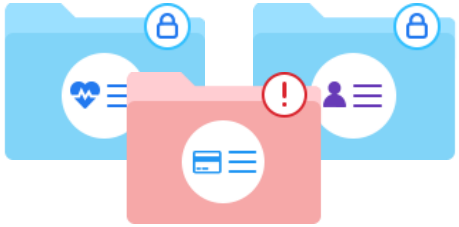
1. Где расположены конфиденциальные данные?
2. У кого есть к ним доступ?
3. Выявлена ли активность, угрожающая конфиденциальным данным?
4. Как классификатор данных помогает соответствовать нормативам?

Где расположены конфиденциальные данные?



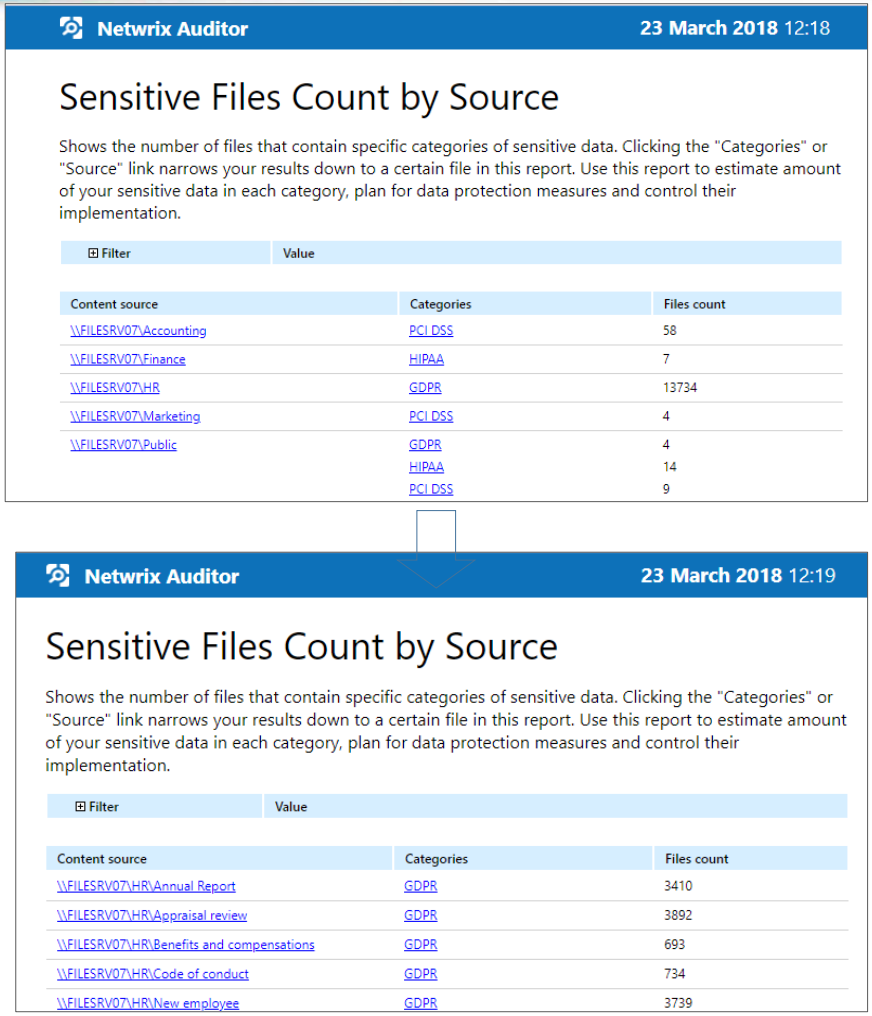
Общий обзор конфиденциальных данных

Приоритетная защита самых важных данных



Выявление данных, находящихся в небезопасных местах

Где расположены конфиденциальные данные?



Netwrix Auditor 23 March 2018 12:18

Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

⊞ Filter | Value

Content source	Categories	Files count
\\FILESRV07\Accounting	PCI DSS	58
\\FILESRV07\Finance	HIPAA	7
\\FILESRV07\HR	GDPR	13734
\\FILESRV07\Marketing	PCI DSS	4
\\FILESRV07\Public	GDPR	4
	HIPAA	14
	PCI DSS	9

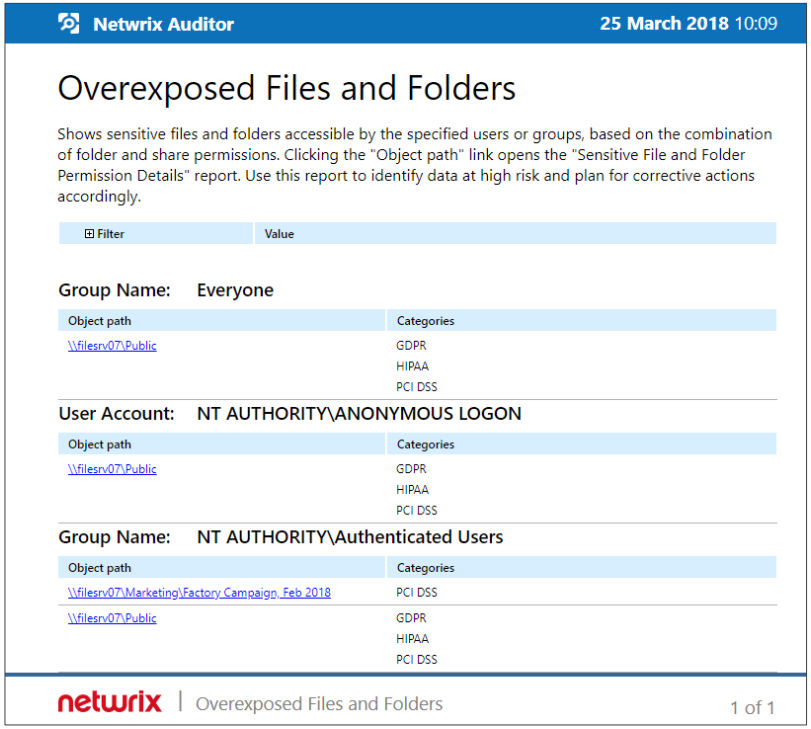
Netwrix Auditor 23 March 2018 12:19

Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

⊞ Filter | Value

Content source	Categories	Files count
\\FILESRV07\HR\Annual Report	GDPR	3410
\\FILESRV07\HR\Appraisal review	GDPR	3892
\\FILESRV07\HR\Benefits and compensations	GDPR	693
\\FILESRV07\HR\Code of conduct	GDPR	734
\\FILESRV07\HR\New employee	GDPR	3739



Netwrix Auditor 25 March 2018 10:09

Overexposed Files and Folders

Shows sensitive files and folders accessible by the specified users or groups, based on the combination of folder and share permissions. Clicking the "Object path" link opens the "Sensitive File and Folder Permission Details" report. Use this report to identify data at high risk and plan for corrective actions accordingly.

⊞ Filter | Value

Group Name: Everyone

Object path	Categories
\\filesrv07\Public	GDPR HIPAA PCI DSS

User Account: NT AUTHORITY\ANONYMOUS LOGON

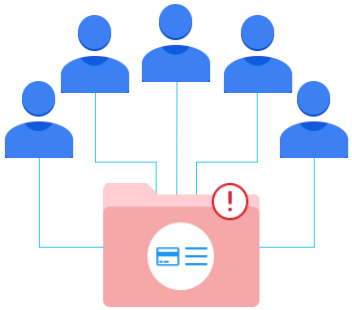
Object path	Categories
\\filesrv07\Public	GDPR HIPAA PCI DSS

Group Name: NT AUTHORITY\Authenticated Users

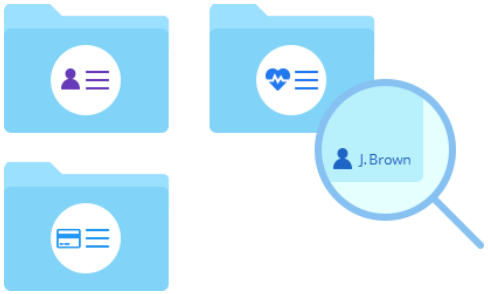
Object path	Categories
\\filesrv07\Marketing\Factory Campaign, Feb 2018	PCI DSS
\\filesrv07\Public	GDPR HIPAA PCI DSS

netwrix | Overexposed Files and Folders 1 of 1

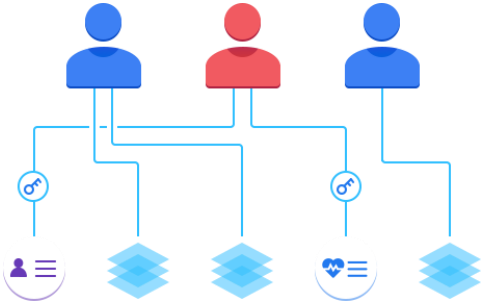
У кого есть доступ к конфиденциальным данным?



Выявление избыточных прав на конфиденциальные данные

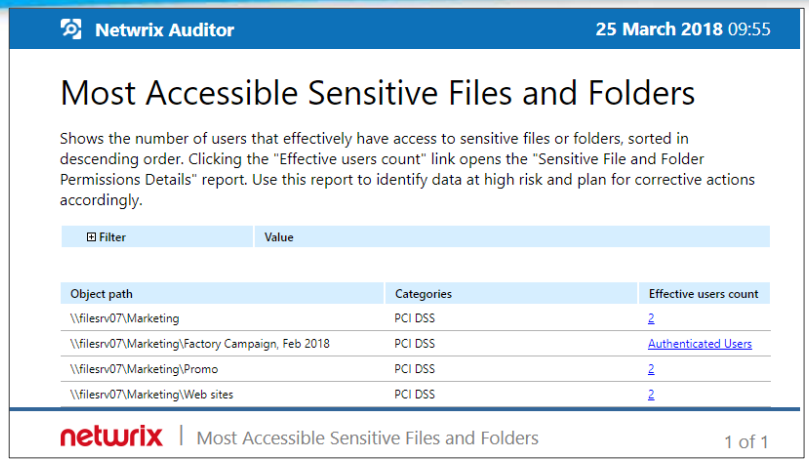


Определение владельцев конфиденциальных данных



Процедура выдачи прав доступа к конфиденциальным данным

У кого есть доступ к конфиденциальным данным?



Netwrix Auditor 25 March 2018 09:55

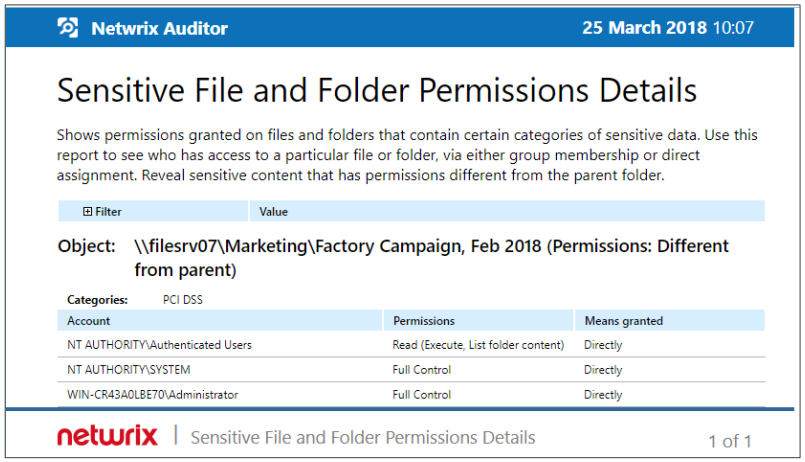
Most Accessible Sensitive Files and Folders

Shows the number of users that effectively have access to sensitive files or folders, sorted in descending order. Clicking the "Effective users count" link opens the "Sensitive File and Folder Permissions Details" report. Use this report to identify data at high risk and plan for corrective actions accordingly.

⊞ Filter	Value

Object path	Categories	Effective users count
\\filesrv07\Marketing	PCI DSS	2
\\filesrv07\Marketing\Factory Campaign, Feb 2018	PCI DSS	Authenticated Users
\\filesrv07\Marketing\Promo	PCI DSS	2
\\filesrv07\Marketing\Web sites	PCI DSS	2

netwrix | Most Accessible Sensitive Files and Folders 1 of 1



Netwrix Auditor 25 March 2018 10:07

Sensitive File and Folder Permissions Details

Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, via either group membership or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

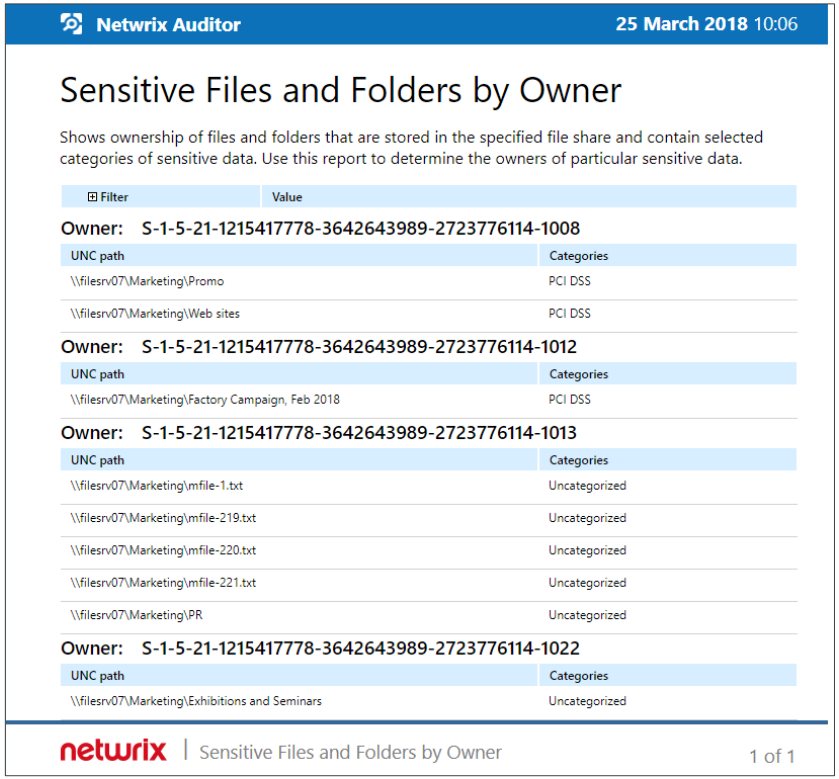
⊞ Filter	Value

Object: \\filesrv07\Marketing\Factory Campaign, Feb 2018 (Permissions: Different from parent)

Categories: PCI DSS

Account	Permissions	Means granted
NT AUTHORITY\Authenticated Users	Read (Execute, List folder content)	Directly
NT AUTHORITY\SYSTEM	Full Control	Directly
WIN-CR43A0LBE70\Administrator	Full Control	Directly

netwrix | Sensitive File and Folder Permissions Details 1 of 1



Netwrix Auditor 25 March 2018 10:06

Sensitive Files and Folders by Owner

Shows ownership of files and folders that are stored in the specified file share and contain selected categories of sensitive data. Use this report to determine the owners of particular sensitive data.

⊞ Filter	Value

Owner: S-1-5-21-1215417778-3642643989-2723776114-1008

UNC path	Categories
\\filesrv07\Marketing\Promo	PCI DSS
\\filesrv07\Marketing\Web sites	PCI DSS

Owner: S-1-5-21-1215417778-3642643989-2723776114-1012

UNC path	Categories
\\filesrv07\Marketing\Factory Campaign, Feb 2018	PCI DSS

Owner: S-1-5-21-1215417778-3642643989-2723776114-1013

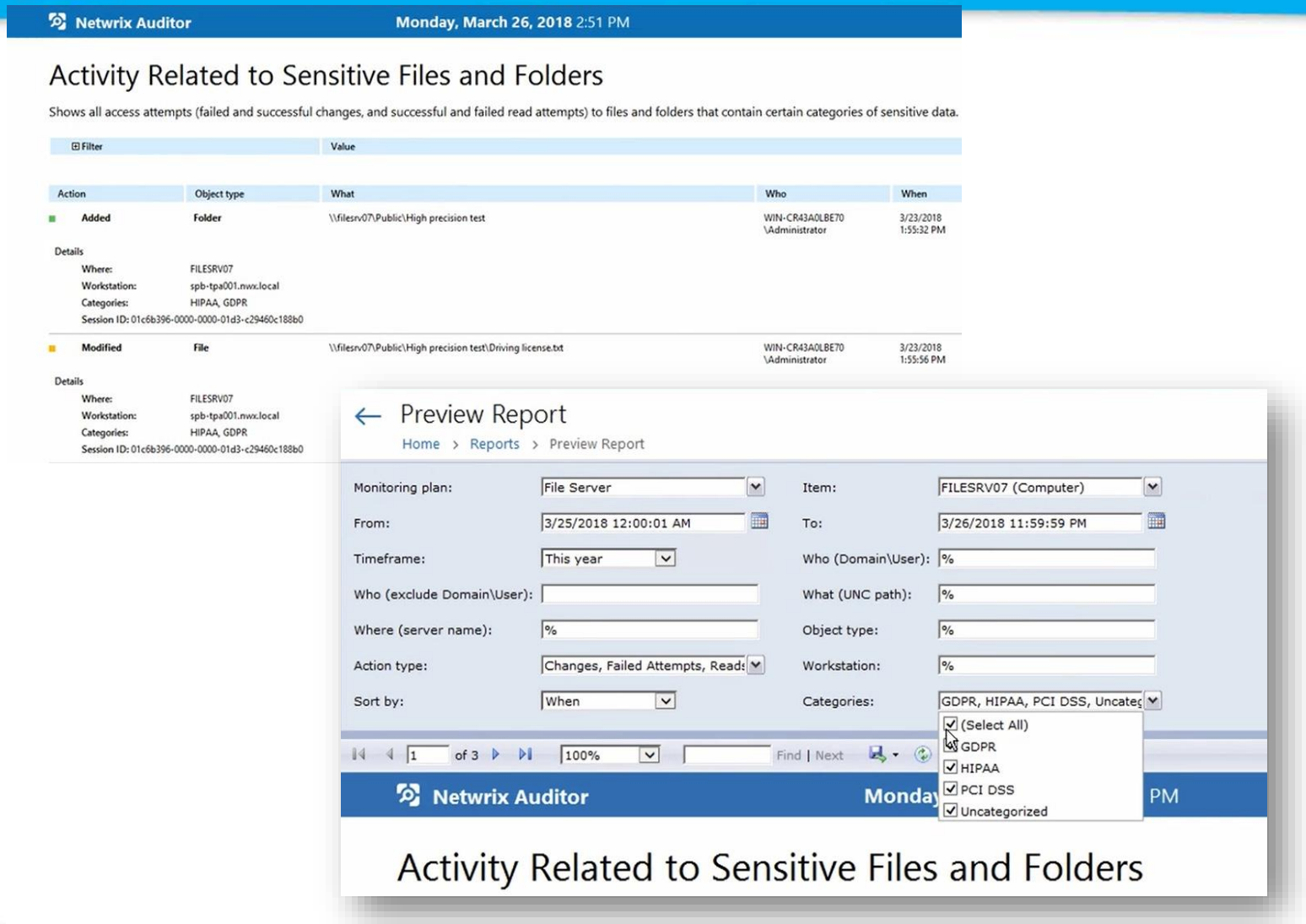
UNC path	Categories
\\filesrv07\Marketing\mfile-1.txt	Uncategorized
\\filesrv07\Marketing\mfile-219.txt	Uncategorized
\\filesrv07\Marketing\mfile-220.txt	Uncategorized
\\filesrv07\Marketing\mfile-221.txt	Uncategorized
\\filesrv07\Marketing\PR	Uncategorized

Owner: S-1-5-21-1215417778-3642643989-2723776114-1022

UNC path	Categories
\\filesrv07\Marketing\Exhibitions and Seminars	Uncategorized

netwrix | Sensitive Files and Folders by Owner 1 of 1

Выявлены ли угрозы конфиденциальным данным?



Классификация данных и нормативы

Sensitive File and Folder Permissions Details

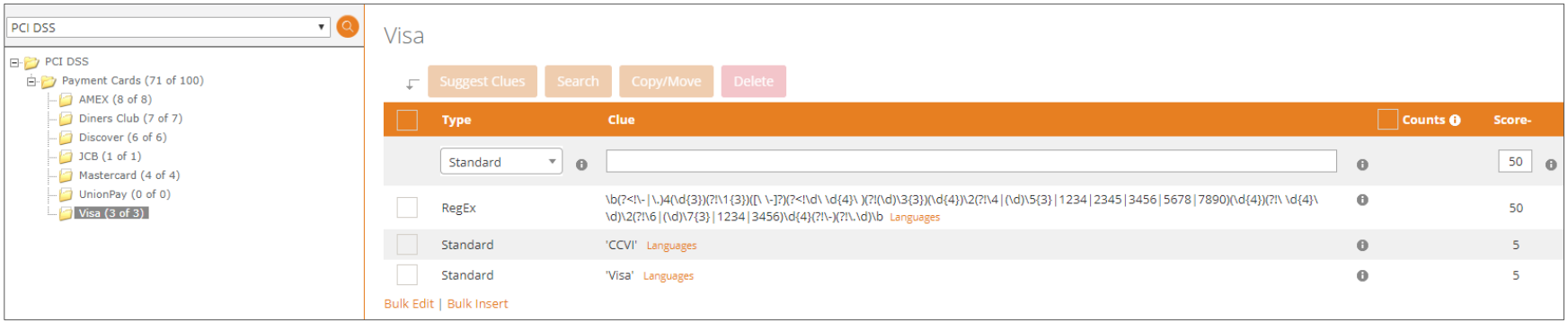
Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, via either group membership or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

Object: \\fs1\Accounting (Permissions: Different from parent)
Categories: GDPR, PCI DSS

Account	Permissions	Means granted
ENTERPRISE\J.Carter	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
ENTERPRISE\A.Brown	Full Control	Group

Object: \\fs1\Accounting\Europe (Permissions: Different from parent)
Categories: GDPR

Account	Permissions	Means granted
ENTERPRISE\M.Smith	Full Control	Group
ENTERPRISE\A.Gold	Full Control	Group



Netwrix Auditor for File Servers

мониторинг изменений на файловых серверах

5 Сценариев

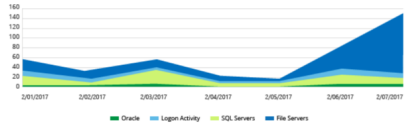
netwrix

+7 812 309 54 98

5 отчетов в Netwrix Auditor для обнаружения атак на файловые сервера

Failed Activity Trend

Shows consolidated statistics on failed actions, including failed read attempts, failed modification attempts, failed logons, etc. The report also lists the users with most failed attempts.



Date: 2/07/2017 (Attempts: 150)

Who	Attempts
ENTERPRISE\D.Harris	78
ENTERPRISE\G.Brown	50
ENTERPRISE\T.Simpson	22

1 Тренды неудачных активностей (Failed activity trend)

Оперативно обнаруживайте многократные неудачные попытки пользователей залогиниться или прочитать, изменить, удалить файлы или папки, чтобы предотвратить атаку и утечку критических данных вашей организации.

Netwrix Auditor позволяет легко обнаруживать пики неудачной активности в ваших файловых серверах и других критических для бизнеса системах, а также позволяет расследовать тренды активности пользователей с наибольшим количеством неудачных действий.

2 Изменения в правах доступа (Changes to access permissions)

Взломщики ничего не сделают с вашими данными, пока не получат определенный уровень доступа к ним. Поэтому после взлома системы они пытаются взломать привилегированные аккаунты, чтобы получить необходимый уровень доступа к данным.

Не допускайте превышения привилегий, отслеживая изменения в правах доступа на ваших файловых серверах и обнаруживая все случаи, когда пользователям раздаются привилегии без рабочей необходимости.

Permission Changes

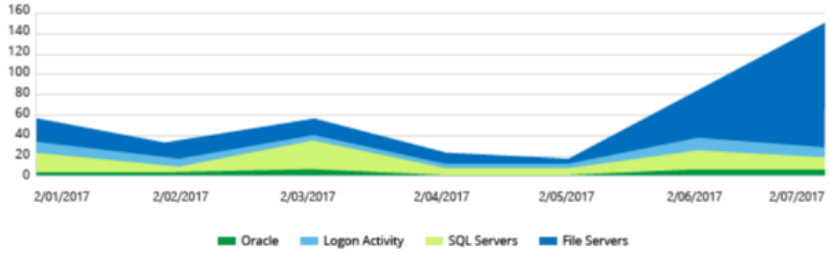
Shows changes in file, folder, and share permissions for a specified period of time. This report must be reviewed on a regular basis to detect unauthorized access and verify that only allowed groups of people have access to sensitive data.

Action	Object type	What	Who	When
Modified	Folder	\\fs1\Office\Management	ENTERPRISE\J.Smith	2/07/2017 3:14:11 PM
Where: fs1 Permissions: • Added: "ENTERPRISE\E.Nelson (Allow: Create files / write data, Create folders / append data, Write extended attributes, Write attributes) Apply onto: This folder only"				
Modified	File	\\fs1\Office\Marketing\Strategy.docx	ENTERPRISE\K.Brown	2/07/2017 1:44:51 PM
Where: fs1 Permissions: • Added: "ENTERPRISE\T.Lee (Allow: Create files / write data, Create folders / append data, Write extended attributes, Write attributes)"				

Тренды неудачных активностей

Failed Activity Trend

Shows consolidated statistics on failed actions, including failed read attempts, failed modification attempts, failed logons, etc. The report also lists the users with most failed attempts.



Date: 2/07/2017 (Attempts: 150)

Who	Attempts
ENTERPRISE\D.Harris	78
ENTERPRISE\G.Brown	50
ENTERPRISE\T.Simpson	22

1 Тренды неудачных активностей (Failed activity trend)

Оперативно обнаруживайте многократные неудачные попытки пользователей залогиниться или прочитать, изменить, удалить файлы или папки, чтобы предотвратить атаку и утечку критических данных вашей организации.

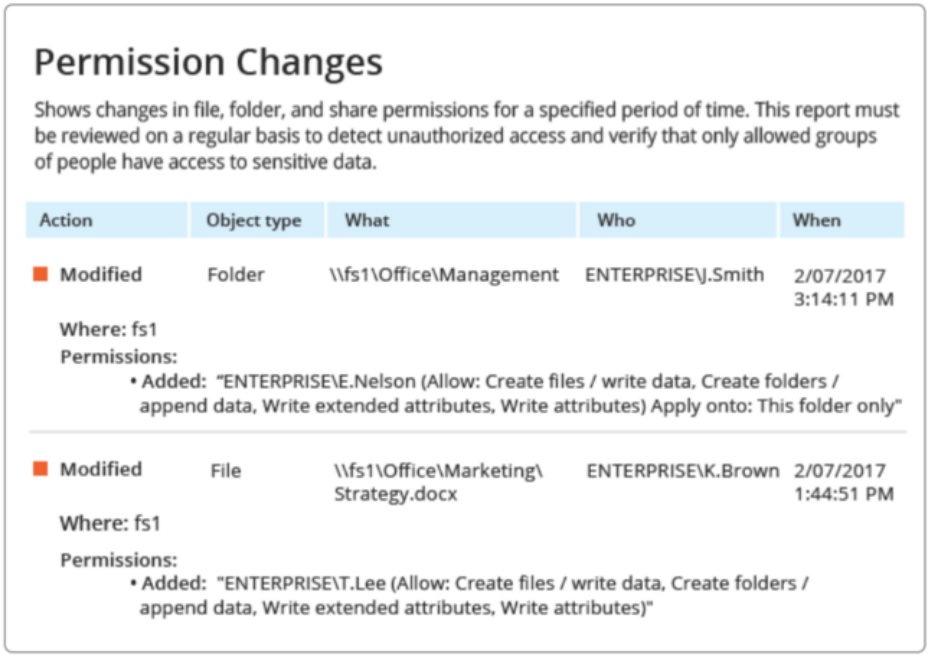
Netwrix Auditor позволяет легко обнаруживать пики неудачной активности в ваших файловых серверах и других критических для бизнеса системах, а также позволяет расследовать тренды активности пользователей с наибольшим количеством неудачных действий.

Изменение прав доступа

2 Изменения в правах доступа (Changes to access permissions)

Взломщики ничего не сделают с вашими данными, пока не получат определенный уровень доступа к ним. Поэтому после взлома системы они пытаются взломать привилегированные аккаунты, чтобы получить необходимый уровень доступа к данным.

Не допускайте превышения привилегий, отслеживая изменения в правах доступа на ваших файловых серверах и обнаруживая все случаи, когда пользователям раздаются привилегии без рабочей необходимости.



Permission Changes

Shows changes in file, folder, and share permissions for a specified period of time. This report must be reviewed on a regular basis to detect unauthorized access and verify that only allowed groups of people have access to sensitive data.

Action	Object type	What	Who	When
Modified	Folder	\\fs1\Office\Management	ENTERPRISE\J.Smith	2/07/2017 3:14:11 PM

Where: fs1
Permissions:
• Added: "ENTERPRISE\E.Nelson (Allow: Create files / write data, Create folders / append data, Write extended attributes, Write attributes) Apply onto: This folder only"

Action	Object type	What	Who	When
Modified	File	\\fs1\Office\Marketing\ Strategy.docx	ENTERPRISE\K.Brown	2/07/2017 1:44:51 PM

Where: fs1
Permissions:
• Added: "ENTERPRISE\T.Lee (Allow: Create files / write data, Create folders / append data, Write extended attributes, Write attributes)"

Всплески активности с данными

Data Access Surges

Shows users who have accessed sensitive data they almost never accessed before (by default, the inactivity threshold is set to 2 actions). The report highlights previously inactive users who performed more actions within a short period of time (by default, 7 days) than during a considerably longer preceding period (by default, 30 days).

Path	User Name	Attempts
\\fs1\Office\Finance\Cardholders.xlsx	ENTERPRISE\J.Smith	19
http://spenterprise/Documents/Legal/Social Security Numbers.xlsx	ENTERPRISE\G.Johnson	11
\\emcfs2\Office\Accounting\Budget2016.xlsx	ENTERPRISE\J.Rosenberg	6
http://spenterprise/Documents/Accounting/Budget2016.docx	ENTERPRISE\J.Rosenberg	3
\\nf1\Marketing\Backup\Passwords.txt	ENTERPRISE\D.Harris	2

3 Всплески активности с данными (Data access surges)

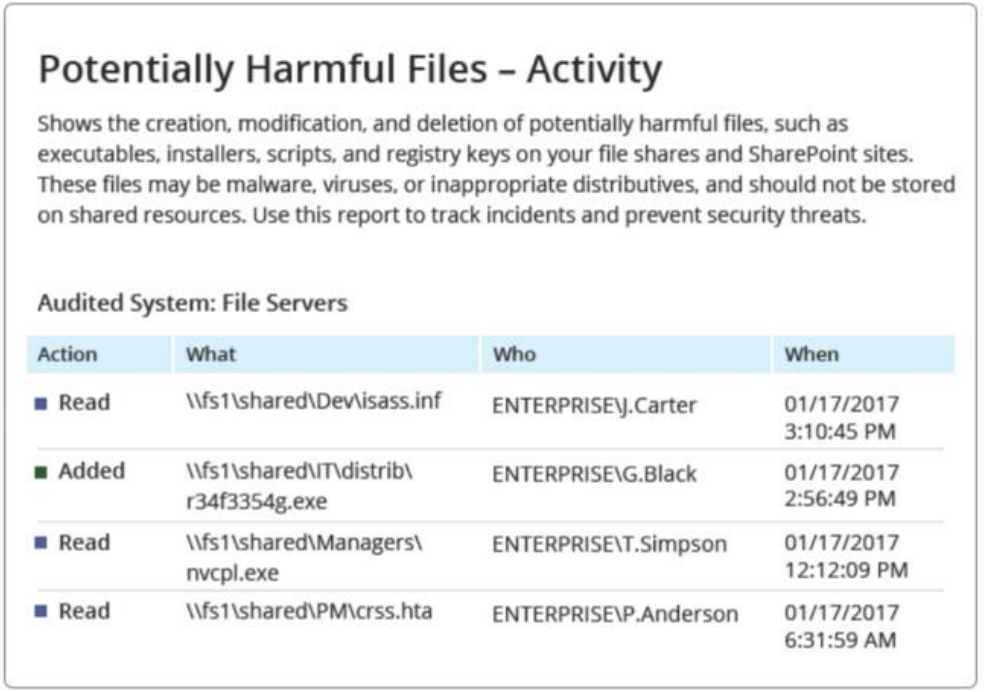
Взломщики часто используют неактивные учетки, чтобы получить доступ к конфиденциальным данным или совершить другие действия незаметно.

Netwrix Auditor позволяет обнаружить действия пользователей, которые ранее были неактивны в течение долгого времени. Таким образом, вы можете блокировать эти аккаунты и пресечь вторжение в систему.

Активность с потенциально опасными файлами

4 Активность с потенциально опасными файлами (Potentially harmful files activity)

Во многих случаях взломщики действуют не вручную; они используют определенные файлы, чтобы произвести массовую атаку на ваши файловые сервера и зашифровать ваши файлы, удалить конфиденциальную информацию или скопировать информацию на свои сервера. **Netwrix Auditor отслеживает подозрительные расширения файлов, которые могут оказаться вредоносными или опасными.** Мы советуем подписаться на такой отчет и просматривать его ежедневно, чтобы вы смогли моментально блокировать такие файлы.



Potentially Harmful Files – Activity

Shows the creation, modification, and deletion of potentially harmful files, such as executables, installers, scripts, and registry keys on your file shares and SharePoint sites. These files may be malware, viruses, or inappropriate distributives, and should not be stored on shared resources. Use this report to track incidents and prevent security threats.

Audited System: File Servers

Action	What	Who	When
Read	\\fs1\shared\Dev\isass.inf	ENTERPRISE\J.Carter	01/17/2017 3:10:45 PM
Added	\\fs1\shared\IT\distrib\r34f3354g.exe	ENTERPRISE\G.Black	01/17/2017 2:56:49 PM
Read	\\fs1\shared\Managers\nvcpl.exe	ENTERPRISE\T.Simpson	01/17/2017 12:12:09 PM
Read	\\fs1\shared\PM\crss.hta	ENTERPRISE\P.Anderson	01/17/2017 6:31:59 AM

Активность в нерабочее время

Potentially Harmful Files – Activity

Shows the creation, modification, and deletion of potentially harmful files, such as executables, installers, scripts, and registry keys on your file shares and SharePoint sites. These files may be malware, viruses, or inappropriate distributives, and should not be stored on shared resources. Use this report to track incidents and prevent security threats.

Audited System: File Servers

Action	What	Who	When
Read	\\fs1\shared\Dev\isass.inf	ENTERPRISE\J.Carter	01/17/2017 3:10:45 PM
Added	\\fs1\shared\IT\distrib\ r34f3354g.exe	ENTERPRISE\G.Black	01/17/2017 2:56:49 PM
Read	\\fs1\shared\Managers\ nvcpl.exe	ENTERPRISE\T.Simpson	01/17/2017 12:12:09 PM
Read	\\fs1\shared\PM\crss.hta	ENTERPRISE\P.Anderson	01/17/2017 6:31:59 AM

5 Активность в нерабочее время (Activity outside business hours)

Если сотрудник логинится в корпоративный аккаунт и работает с данными в нерабочее время, это может вызвать сомнения и необходимость в проверке.

Оперативно узнавайте обо всех действиях в нерабочее время, как только они совершаются, и быстро обнаруживайте инсайдерские атаки или взломщиков.

Пример отчета: активность на файловом сервере

All File Server Activity

Shows activity (changes, failed modifications, reads and failed read attempts) on all audited file servers.

Action	Object type	What	Who	When
Removed	File	\\fs1\Office\Finance\ Order231.docx	ENTERPRISE\J.Brown	7/15/2015 1:20:39 PM
Where: ENTWKS0343				
Added	Folder	\\fs1\Office\Accounting\ Invoices	ENTERPRISE\J.Brown	7/15/2015 2:11:41 PM
Where: ENTWKS0343				
Modified	File	\\fs1\Office\Marketing\ advert_campaign.pptx	ENTERPRISE\N.King	7/15/2015 2:20:14 PM
Where: 172.17.5.12				

- Кто/Что/Когда/Где сделал
- Фильтр и шаблоны *.*
- Подписка на отчеты
- Оповещения о попытках копирования/чтения/изменения
- Мониторинг действий: Чтение/Создание/Удаление/Изменений
- Неудачные попытки доступа/изменения
- Экспорт в форматы csv/word/excel/pdf

Статистика по действиям на файловом сервере

Preview Report

Managed Object:	File Server Fast, File Server Full	Timeframe:	Specific dates
From:	4/28/2014 12:00:01 AM	To:	4/29/2016 11:59:59 PM
Who (Domain\User):	%	Who (Exclude Domain\User):	
What (UNC Path):	%	Changes per User (Lower Limit):	100
Reads per User (Lower Limit):	0	Failed Attempts per User (Lower Limit):	0
Deletions per User (Lower Limit):	0	Sort By:	Who

1 of 1 | 100% | Find | Next

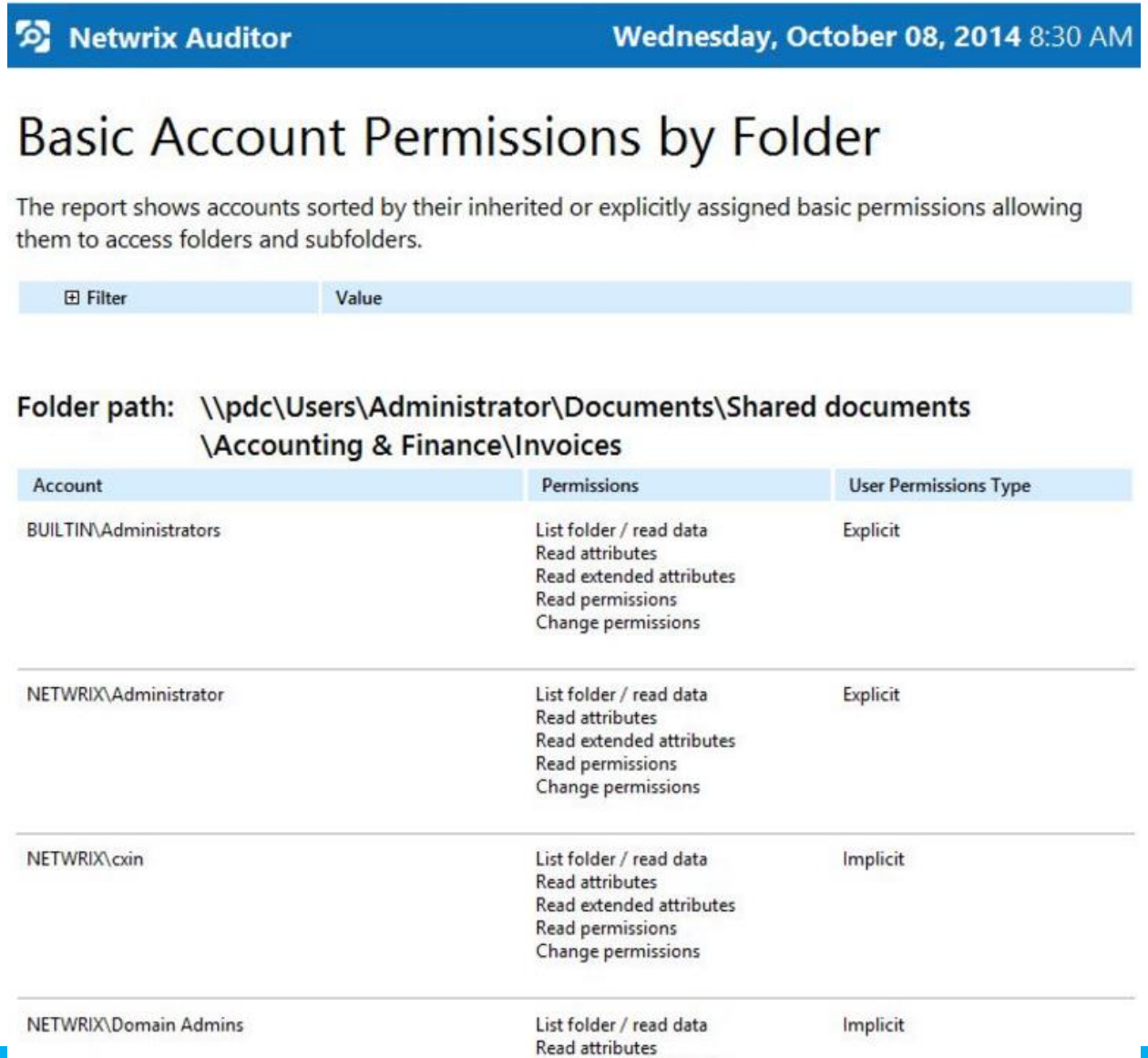
User Activity Summary

Shows the most active users. Use this report to detect suspicious user activity such as high numbers of failed access attempts or file reads.

⊞ Filter	Value

Who	Changes	Reads	Failed Attempts	Deletions
DNWX5\a.mozart	109	21	38	14
DNWX5\a.tkach	573	21	0	37
DNWX5\Administrator	126	0	0	4
DNWX5\e.presley	132	148	528	24
DNWX5\NetwrixSvc	116	260	0	15

Пример отчета: матрица прав доступа



Netwrix Auditor — Wednesday, October 08, 2014 8:30 AM

Basic Account Permissions by Folder

The report shows accounts sorted by their inherited or explicitly assigned basic permissions allowing them to access folders and subfolders.

⊞ Filter	Value

Folder path: \\pdc\Users\Administrator\Documents\Shared documents\Accounting & Finance\Invoices

Account	Permissions	User Permissions Type
BUILTIN\Administrators	List folder / read data Read attributes Read extended attributes Read permissions Change permissions	Explicit
NETWRIX\Administrator	List folder / read data Read attributes Read extended attributes Read permissions Change permissions	Explicit
NETWRIX\cxin	List folder / read data Read attributes Read extended attributes Read permissions Change permissions	Implicit
NETWRIX\Domain Admins	List folder / read data Read attributes	Implicit

Пример отчета:
Изменения прав на файлы и папки

Permission Changes

Shows changes in file, folder, and share permissions for a specified period of time. This report must be reviewed on a regular basis to detect unauthorized access and verify that only allowed groups of people have access to sensitive data.

Action	Object type	What	Who	When
Modified	Folder	\\fs1\Office\Management	ENTERPRISE\J.Smith	7/15/2015 1:44:11 PM
Where: ENTWKS0312 **Permissions:** • **Added:** "ENTERPRISE\E.Nelson (Allow: Create files / write data, Create folders / append data, Write extended attributes, Write attributes) Apply onto: This folder only"				
Modified	File	\\fs1\Office\Marketing\ Strategy.docx	ENTERPRISE\K.Brown	7/15/2015 3:14:51 PM
Where: 172.17.2.45 **Permissions:** • **Added:** "ENTERPRISE\T.Lee (Allow: Create files / write data, Create folders / append data, Write extended attributes, Write attributes)"				

Избыточный доступ к ресурсам

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks. Track permissions assigned to accounts directly or by group membership.

Object: \\fs1\Acconting (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\N.Key	Full Control	Directly	0
ENTERPRISE\T.Simpson	Full Control	Group	0
ENTERPRISE\P.Anderson	Full Control	Group	0
ENTERPRISE\K.Miller	Write and List folder content	Directly	0
ENTERPRISE\T.Allen	Read (Execute, List folder content)	Group	

Права выданы «напрямую», не пользовался ни разу

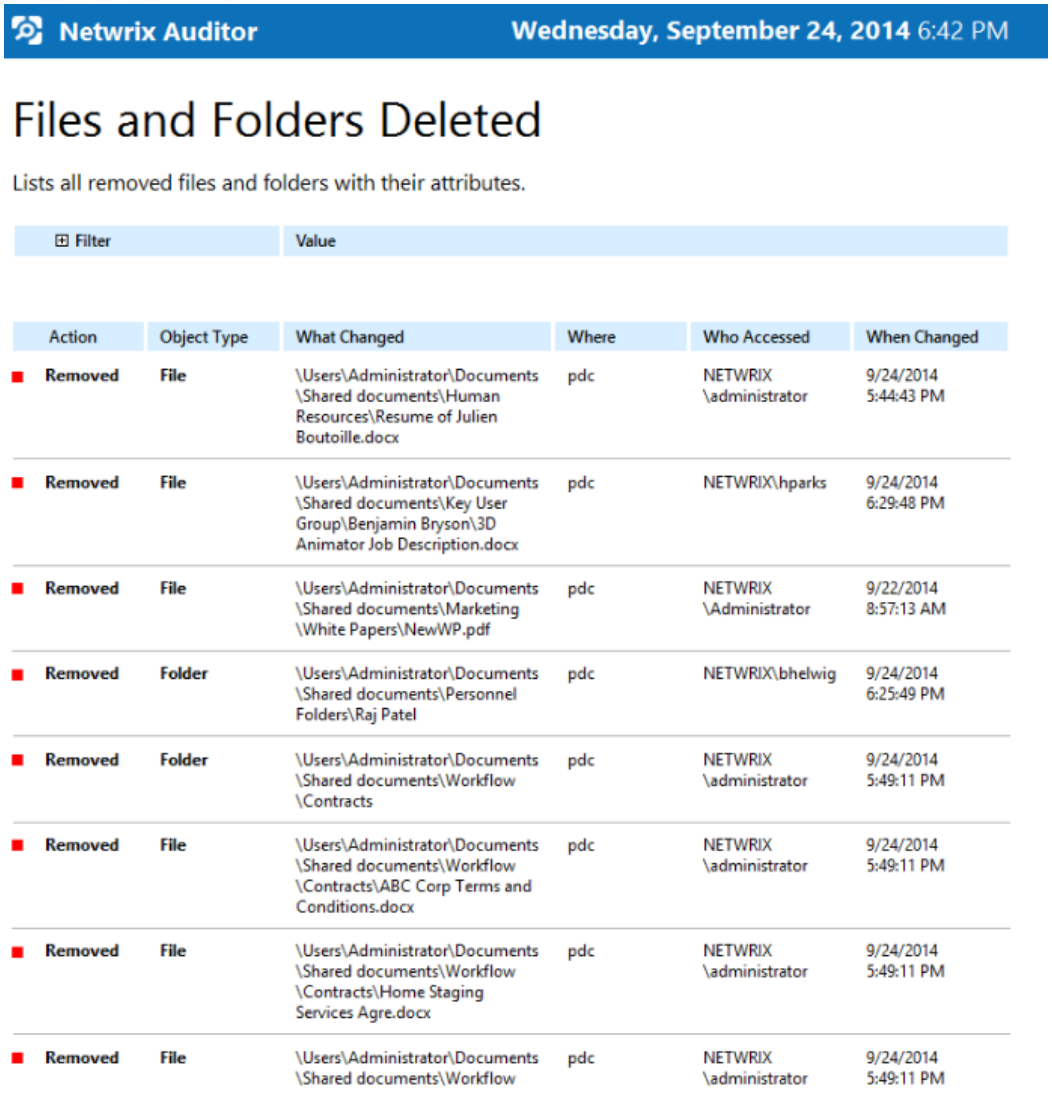
Пример отчета: неудачные попытки чтения

Failed Read Attempts

Shows unauthorized file access attempts. This report can be used for compliance audit to show that all unauthorized data access activities are traceable and easily auditable.

Action	Object Type	What	Who	When
Read (Failed Attempt)	File	\\fs1\Finance\Cardholders\Overview.xlsx	ENTERPRISE\B.Green	9/26/2015 3:03:08 PM
Where:	ENTWKS0412			
Read (Failed Attempt)	File	\\fs1\Finance\Accounting\Statement0313.xlsx	ENTERPRISE\S.Hernandez	9/26/2015 3:05:38 PM
Where:	ENTWKS0524			
Read (Failed Attempt)	File	\\fs1\HR\NewHire\SalaryList.xlsx	ENTERPRISE\K.Davis	9/26/2015 3:07:23 PM
Where:	172.17.4.34			

Пример отчета: удаленные папки и файлы



Netwrix Auditor Wednesday, September 24, 2014 6:42 PM

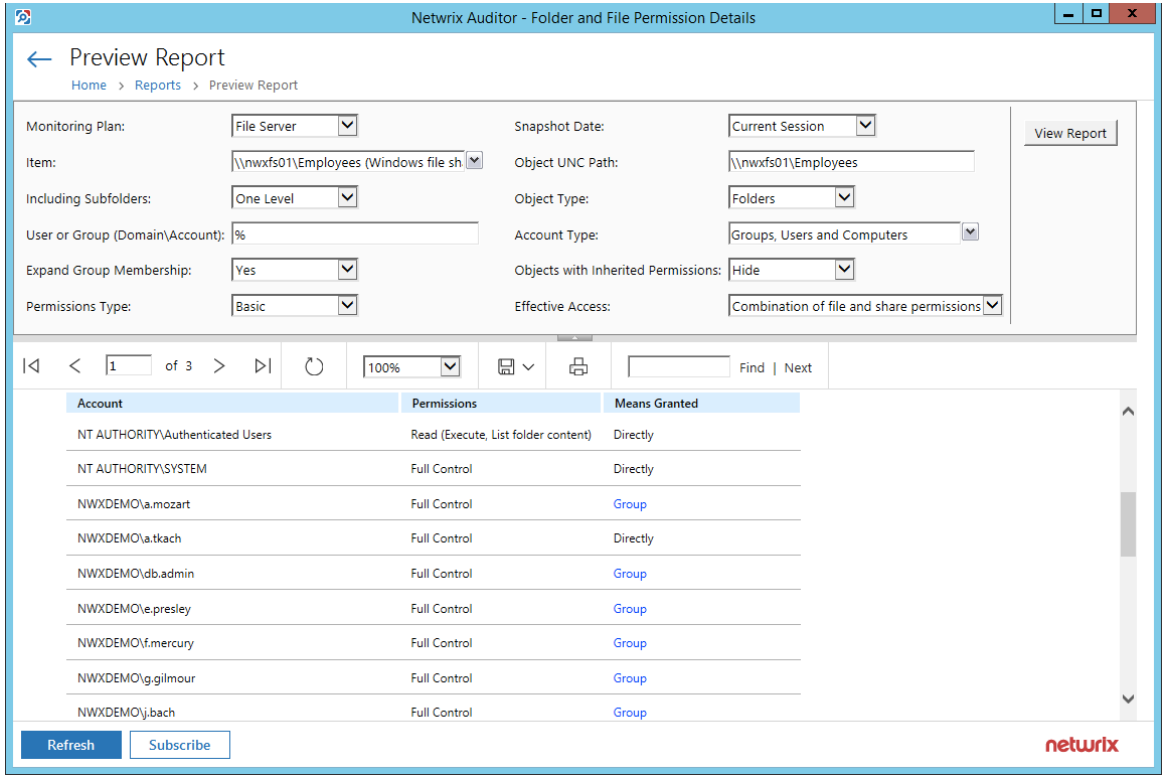
Files and Folders Deleted

Lists all removed files and folders with their attributes.

Filter	Value

Action	Object Type	What Changed	Where	Who Accessed	When Changed
Removed	File	\Users\Administrator\Documents\Shared documents\Human Resources\Resume of Julien Boutoille.docx	pdc	NETWRIX\administrator	9/24/2014 5:44:43 PM
Removed	File	\Users\Administrator\Documents\Shared documents\Key User Group\Benjamin Bryson\3D Animator Job Description.docx	pdc	NETWRIX\hparks	9/24/2014 6:29:48 PM
Removed	File	\Users\Administrator\Documents\Shared documents\Marketing\White Papers\NewWP.pdf	pdc	NETWRIX\Administrator	9/22/2014 8:57:13 AM
Removed	Folder	\Users\Administrator\Documents\Shared documents\Personnel Folders\Raj Patel	pdc	NETWRIX\bhelwig	9/24/2014 6:25:49 PM
Removed	Folder	\Users\Administrator\Documents\Shared documents\Workflow\Contracts	pdc	NETWRIX\administrator	9/24/2014 5:49:11 PM
Removed	File	\Users\Administrator\Documents\Shared documents\Workflow\Contracts\ABC Corp Terms and Conditions.docx	pdc	NETWRIX\administrator	9/24/2014 5:49:11 PM
Removed	File	\Users\Administrator\Documents\Shared documents\Workflow\Contracts\Home Staging Services Agre.docx	pdc	NETWRIX\administrator	9/24/2014 5:49:11 PM
Removed	File	\Users\Administrator\Documents\Shared documents\Workflow	pdc	NETWRIX\administrator	9/24/2014 5:49:11 PM

Пример отчета: права доступа



Доступ через группы или напрямую

Включая все дочерние папки

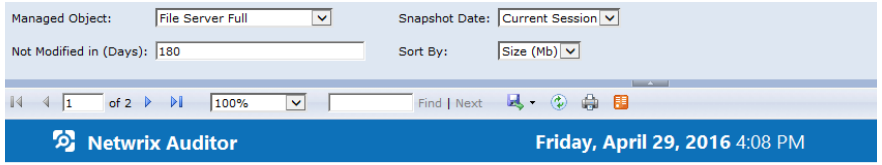
Показывает наследования

Пример отчета: неиспользуемые файлы

Stale Data by Folder

Shows folders containing files with no recent changes (180 days by default). Use this report to identify files and folders that can be safely deleted or moved to archive.

Folder	Owner	Unchanged Files	Unchanged Files Size (MB)
\\fs1\shared\it\2013	ENTERPRISE\Administrators	18	354.0445
\\fs1\Shared\Finance\2014_Reports	ENTERPRISE\S.Bostyn	12	112.5711
\\fs1\Shared\Legal\2015_Contracts	ENTERPRISE\F.Ramirez	42	587.6654
\\fs1\Shared\Sales\2014_Quota	ENTERPRISE\K.Gramberg	38	891.1135



Stale Files List

Shows files with no recent changes. This report is pre-filtered and references the data from the "Stale Data by Folder" report.

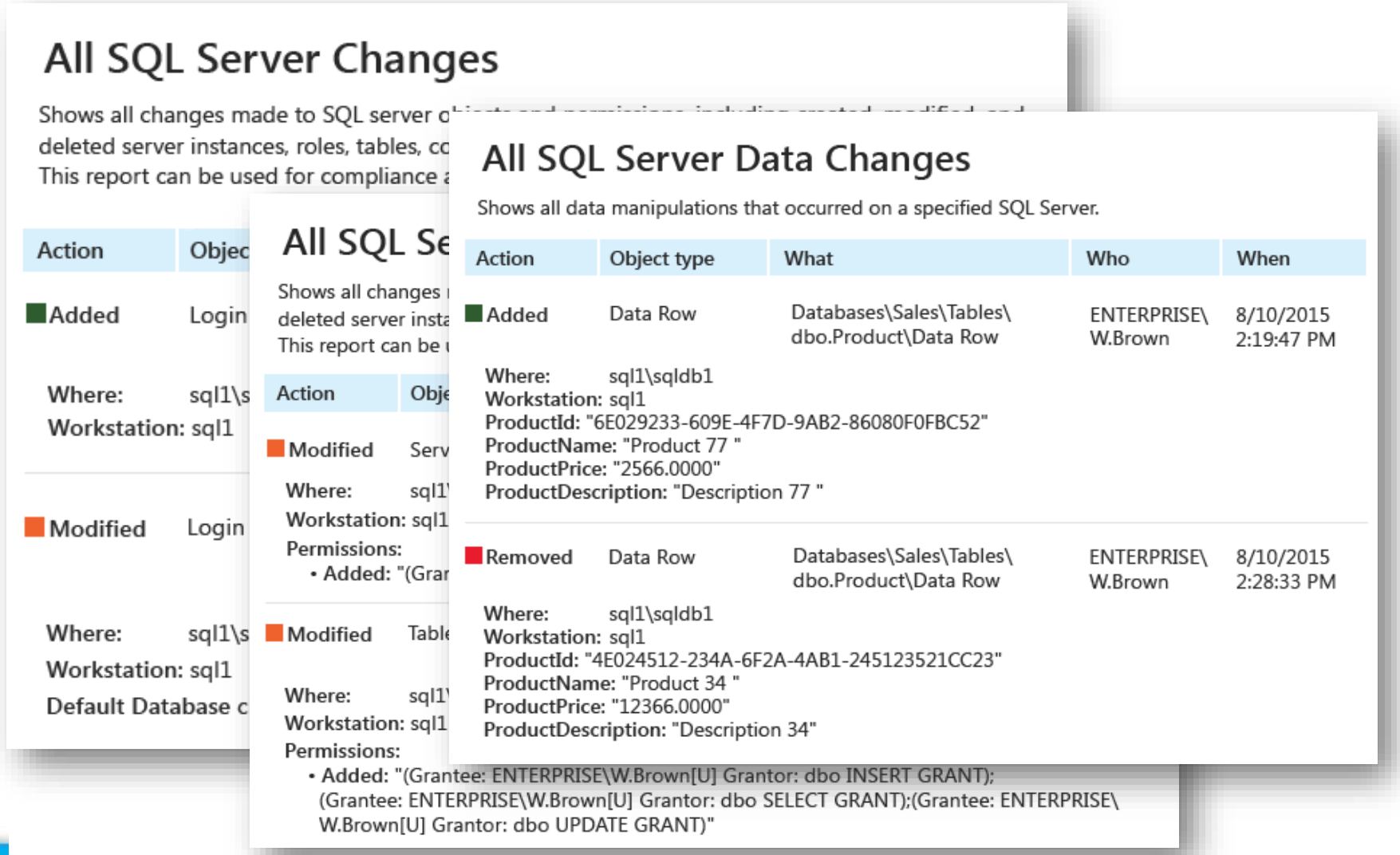
⊞ Filter	Value

Size (MB)	Owner	Path	Created	Modified
57.1250	BUILTIN\Administrators	\\SQL502\data\Mail\Users\Common\340.wav	2/16/2016 10:51:56 PM	2/18/2015 5:54:07 PM
54.1875	BUILTIN\Administrators	\\SQL502\data\Mail\Users\Common\257.wav	2/16/2016 10:51:46 PM	2/18/2015 5:54:05 PM
49.5000	BUILTIN\Administrators	\\SQL502\data\Mail\Users\Common\341.wav	2/16/2016 10:52:00 PM	2/18/2015 5:54:08 PM
48.3125	BUILTIN\Administrators	\\SQL502\data\Mail\Users\Common\258.wav	2/16/2016 10:51:51 PM	2/18/2015 5:54:06 PM
42.4688	BUILTIN\Administrators	\\SQL502\data\Mail\Users\Common\342.wav	2/16/2016 10:52:06 PM	2/18/2015 5:54:09 PM

Модули для SQL, Oracle, Sharepoint, VMware

мониторинг изменений в остальных системах

Примеры отчетов: изменения в Microsoft SQL



All SQL Server Changes

Shows all changes made to SQL server o
deleted server instances, roles, tables, co
This report can be used for compliance a

Action	Objec
Added	Login
Modified	Login

Where: sql1\s
Workstation: sql1

Where: sql1\s
Workstation: sql1
Default Database c

All SQL Se

Shows all changes
deleted server insta
This report can be

Action	Obje
Modified	Serv

Where: sql1
Workstation: sql1
Permissions:
• Added: "(Gran

Modified Table

Where: sql1
Workstation: sql1
Permissions:
• Added: "(Grantee: ENTERPRISE\W.Brown[U] Grantor: dbo INSERT GRANT);
(Grantee: ENTERPRISE\W.Brown[U] Grantor: dbo SELECT GRANT);(Grantee: ENTERPRISE\
W.Brown[U] Grantor: dbo UPDATE GRANT)"

All SQL Server Data Changes

Shows all data manipulations that occurred on a specified SQL Server.

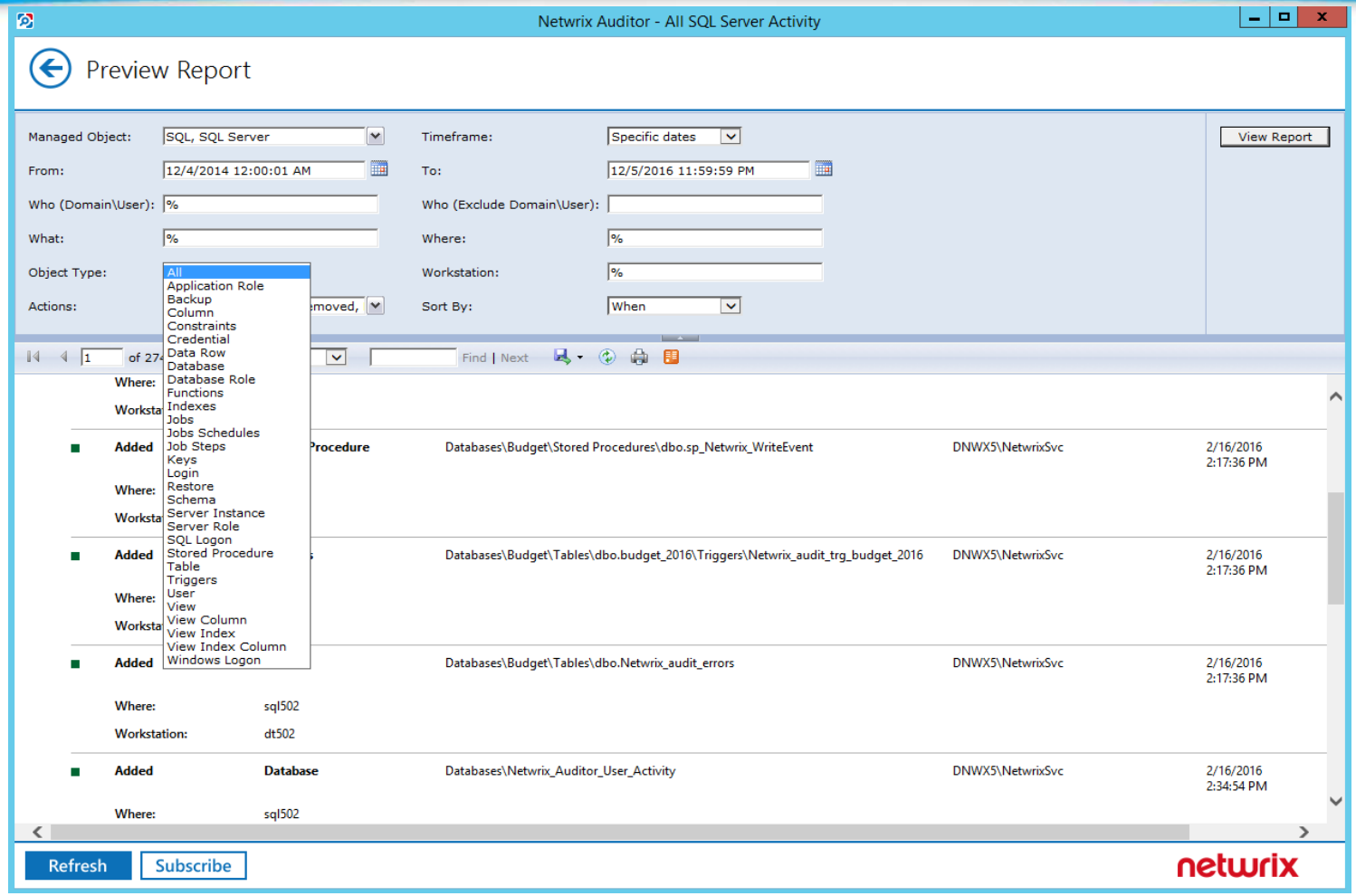
Action	Object type	What	Who	When
Added	Data Row	Databases\Sales\Tables\ dbo.Product\Data Row	ENTERPRISE\ W.Brown	8/10/2015 2:19:47 PM

Where: sql1\sqldb1
Workstation: sql1
ProductId: "6E029233-609E-4F7D-9AB2-86080F0FBC52"
ProductName: "Product 77 "
ProductPrice: "2566.0000"
ProductDescription: "Description 77 "

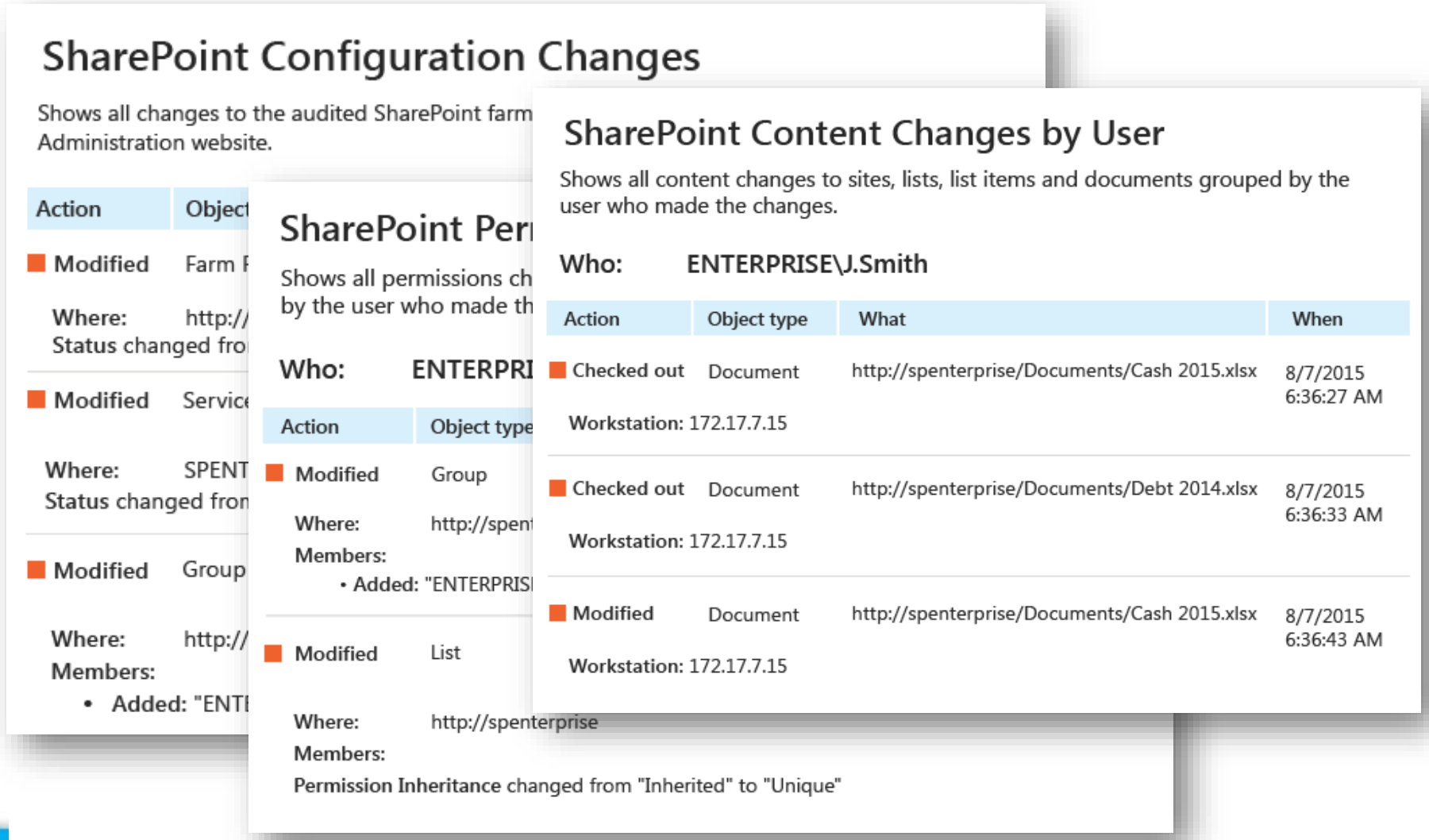
Action	Object type	What	Who	When
Removed	Data Row	Databases\Sales\Tables\ dbo.Product\Data Row	ENTERPRISE\ W.Brown	8/10/2015 2:28:33 PM

Where: sql1\sqldb1
Workstation: sql1
ProductId: "4E024512-234A-6F2A-4AB1-245123521CC23"
ProductName: "Product 34 "
ProductPrice: "12366.0000"
ProductDescription: "Description 34"

Примеры отчетов: выбор типа объектов



Примеры отчетов: изменения в SharePoint



SharePoint Configuration Changes

Shows all changes to the audited SharePoint farm
Administration website.

Action	Object
Modified	Farm
Where:	http://
Status changed fro	
Modified	Service
Where:	SPENT
Status changed fron	
Modified	Group
Where:	http://
Members:	
• Added: "ENTE	

SharePoint Per

Shows all permissions ch
by the user who made th

Who: ENTERPRI

Action	Object type
Modified	Group
Where:	http://spent
Members:	
• Added: "ENTERPRISE	
Modified	List
Where:	http://spenterprise
Members:	

Permission Inheritance changed from "Inherited" to "Unique"

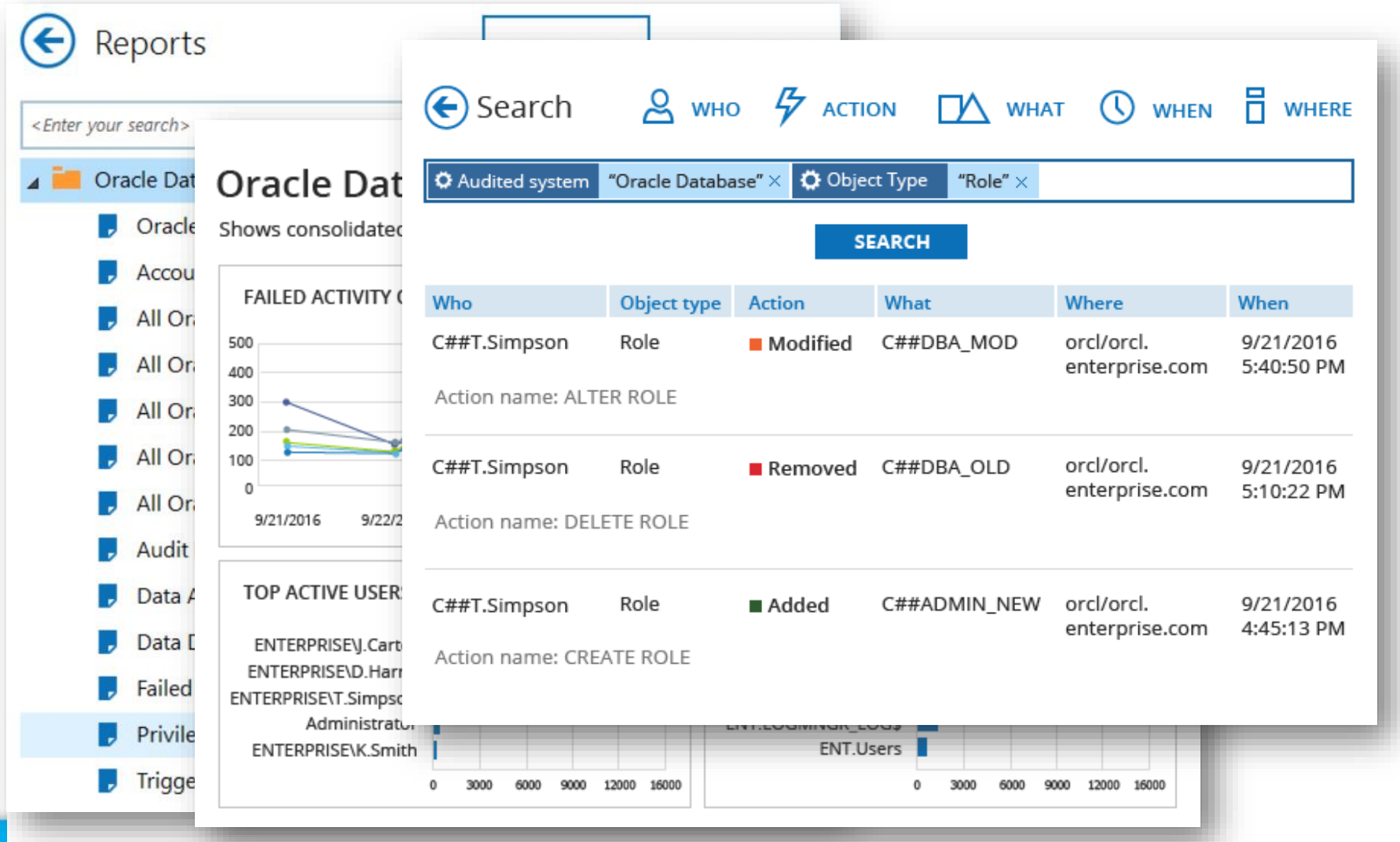
SharePoint Content Changes by User

Shows all content changes to sites, lists, list items and documents grouped by the user who made the changes.

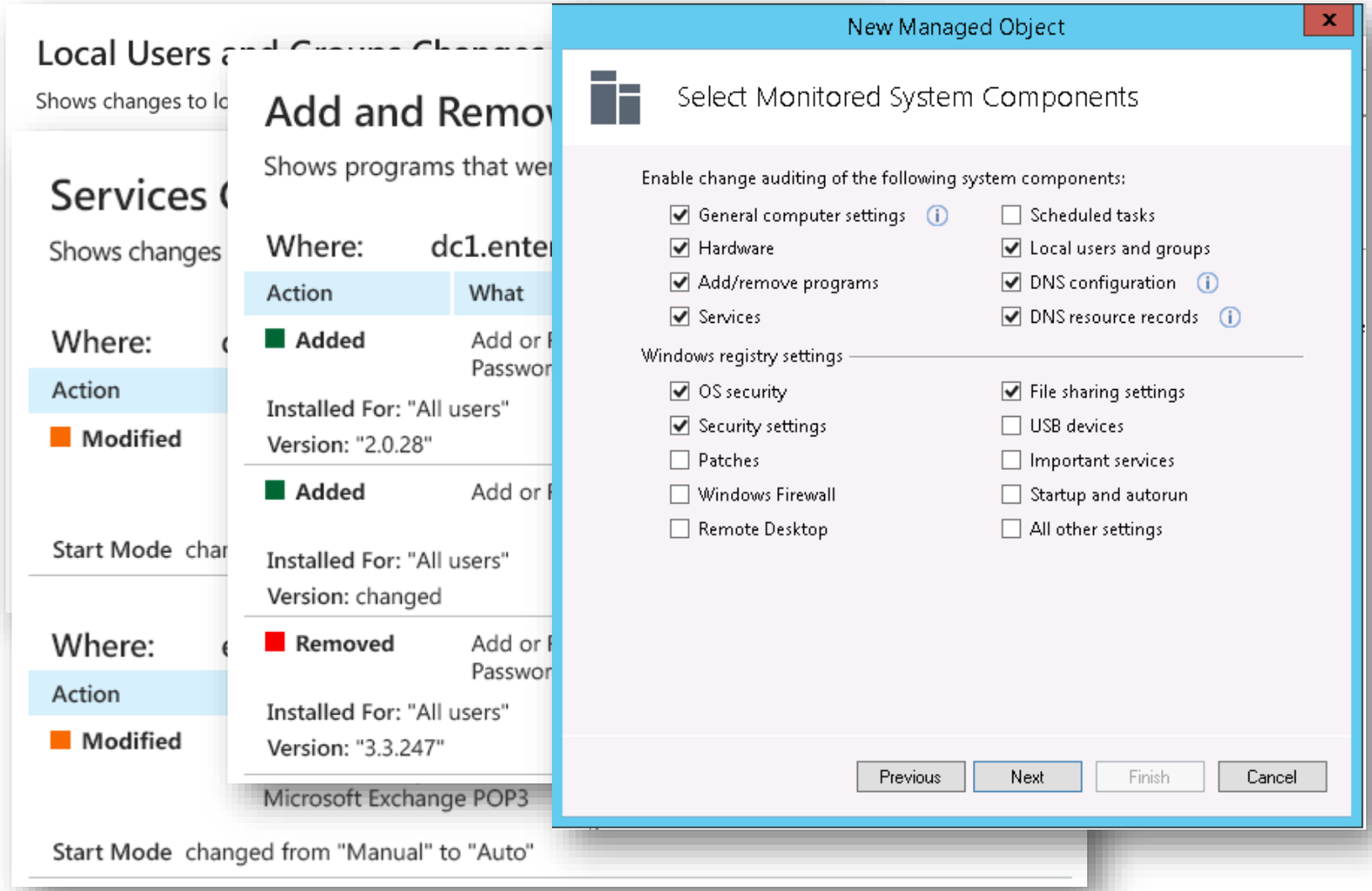
Who: ENTERPRISE\J.Smith

Action	Object type	What	When
Checked out	Document	http://spenterprise/Documents/Cash 2015.xlsx	8/7/2015 6:36:27 AM
Workstation: 172.17.7.15			
Checked out	Document	http://spenterprise/Documents/Debt 2014.xlsx	8/7/2015 6:36:33 AM
Workstation: 172.17.7.15			
Modified	Document	http://spenterprise/Documents/Cash 2015.xlsx	8/7/2015 6:36:43 AM
Workstation: 172.17.7.15			

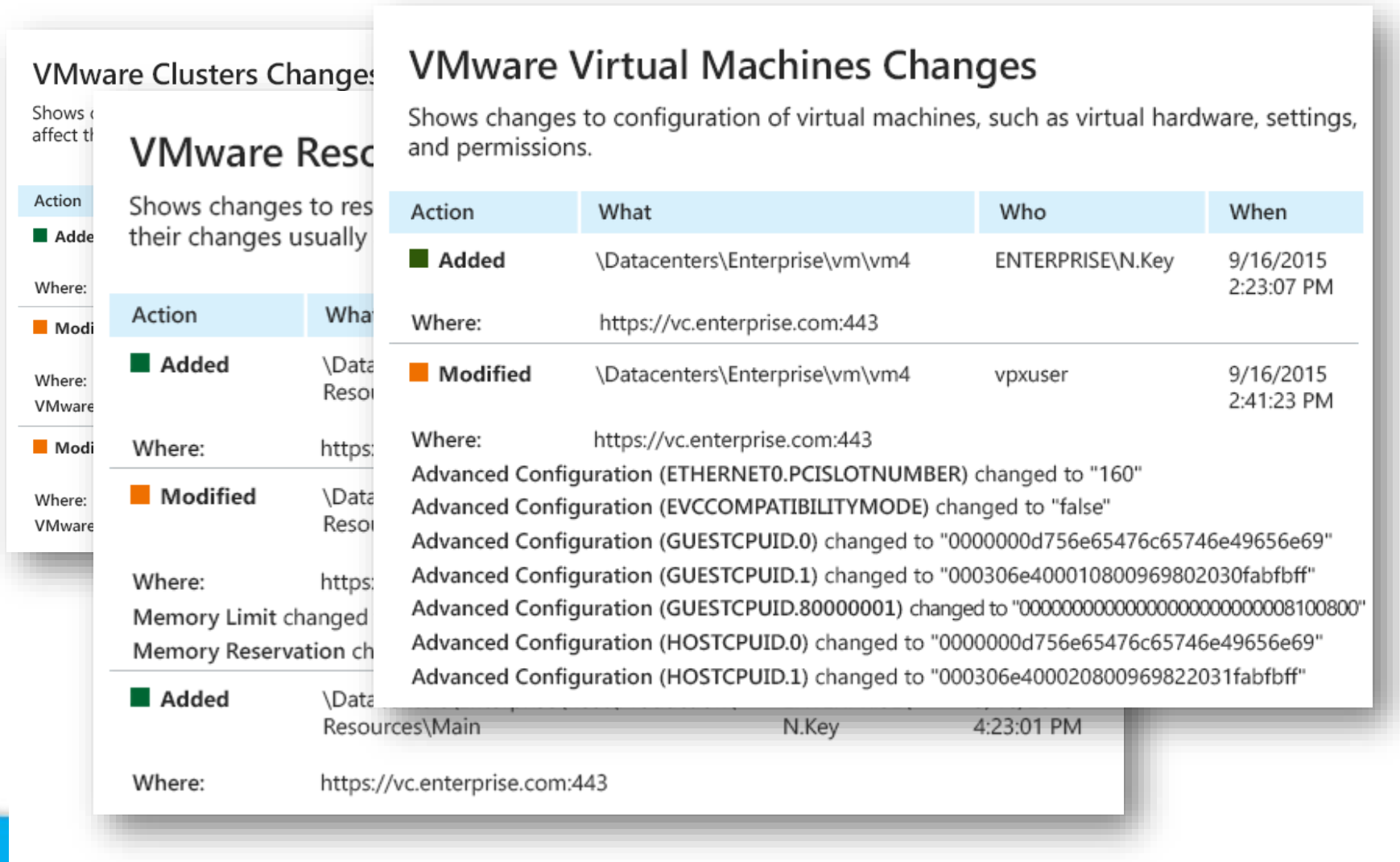
Примеры отчетов: изменения в Oracle Database



Изменения на машинах с Windows



Примеры отчетов: изменения в инфраструктуре



VMware Clusters Changes

Shows
affect th

Action

Added

Where:

Modi

Where:
VMware

Modi

Where:
VMware

VMware Resc

Shows changes to res
their changes usually

Action	What
Added	\Data Resou
Where:	https:
Modified	\Data Resou
Where:	https:
Memory Limit changed	
Memory Reservation ch	
Added	\Data Resources\Main
Where:	https://vc.enterprise.com:443

VMware Virtual Machines Changes

Shows changes to configuration of virtual machines, such as virtual hardware, settings, and permissions.

Action	What	Who	When
Added	\Datacenters\Enterprise\vm\vm4	ENTERPRISE\N.Key	9/16/2015 2:23:07 PM
Where:	https://vc.enterprise.com:443		
Modified	\Datacenters\Enterprise\vm\vm4	vpxuser	9/16/2015 2:41:23 PM
Where:	https://vc.enterprise.com:443		

Advanced Configuration (ETHERNET0.PCISLOTNUMBER) changed to "160"
Advanced Configuration (EVCCOMPATIBILITYMODE) changed to "false"
Advanced Configuration (GUESTCPUID.0) changed to "0000000d756e65476c65746e49656e69"
Advanced Configuration (GUESTCPUID.1) changed to "000306e400010800969802030fabfbff"
Advanced Configuration (GUESTCPUID.80000001) changed to "00000000000000000000000008100800"
Advanced Configuration (HOSTCPUID.0) changed to "0000000d756e65476c65746e49656e69"
Advanced Configuration (HOSTCPUID.1) changed to "000306e400020800969822031fabfbff"

Действия пользователя во всех системах

Netwrix Auditor Tuesday, April 22, 2014 4:39 PM

All Changes by User

Shows all changes across the entire IT infrastructure grouped by the users who made the changes.

Filter	Value

Who Changed: CITY\Megan

Audited System: Active Directory

Action	Object Type	What Changed	Where Changed	When Changed
Modified	User	\local\city\People\Bill	chicago.city.local	3/20/2014 8:35:55 PM
Principal Name set to "Bill@city.local"				
Removed	User	\local\city\People\Sophia	chicago.city.local	3/20/2014 8:36:04 PM

Audited System: Windows Servers

Action	Object Type	What Changed	Where Changed	When Changed
Removed	Registry Key	Registry\HKEY_LOCAL_MACHINE\software\Microsoft\Windows\CurrentVersion\Installer\InProgress	2k8	10/23/2013 6:29:14 PM
(REG_SZ): "C:\Windows\Installer\591ac9.ipi"				
Ownership: "Owner: NT AUTHORITY\SYSTEM"				

Audited System: VMware

Action	Object Type	What Changed	Where Changed	When Changed
Removed	VirtualMachine	\ha-folder-root\ha-datacenter\vm\kn	https://10.0.4.48:443	10/25/2013 6:38:42 PM

Audited System: SQL Servers

Action	Object Type	What Changed	Where Changed	When Changed
Added	Database	Databases\fj	w2012dc1	10/24/2013 9:19:28 PM

Netwrix Auditor Thursday, April 10, 2014 7:01 AM

All Changes by Audited System

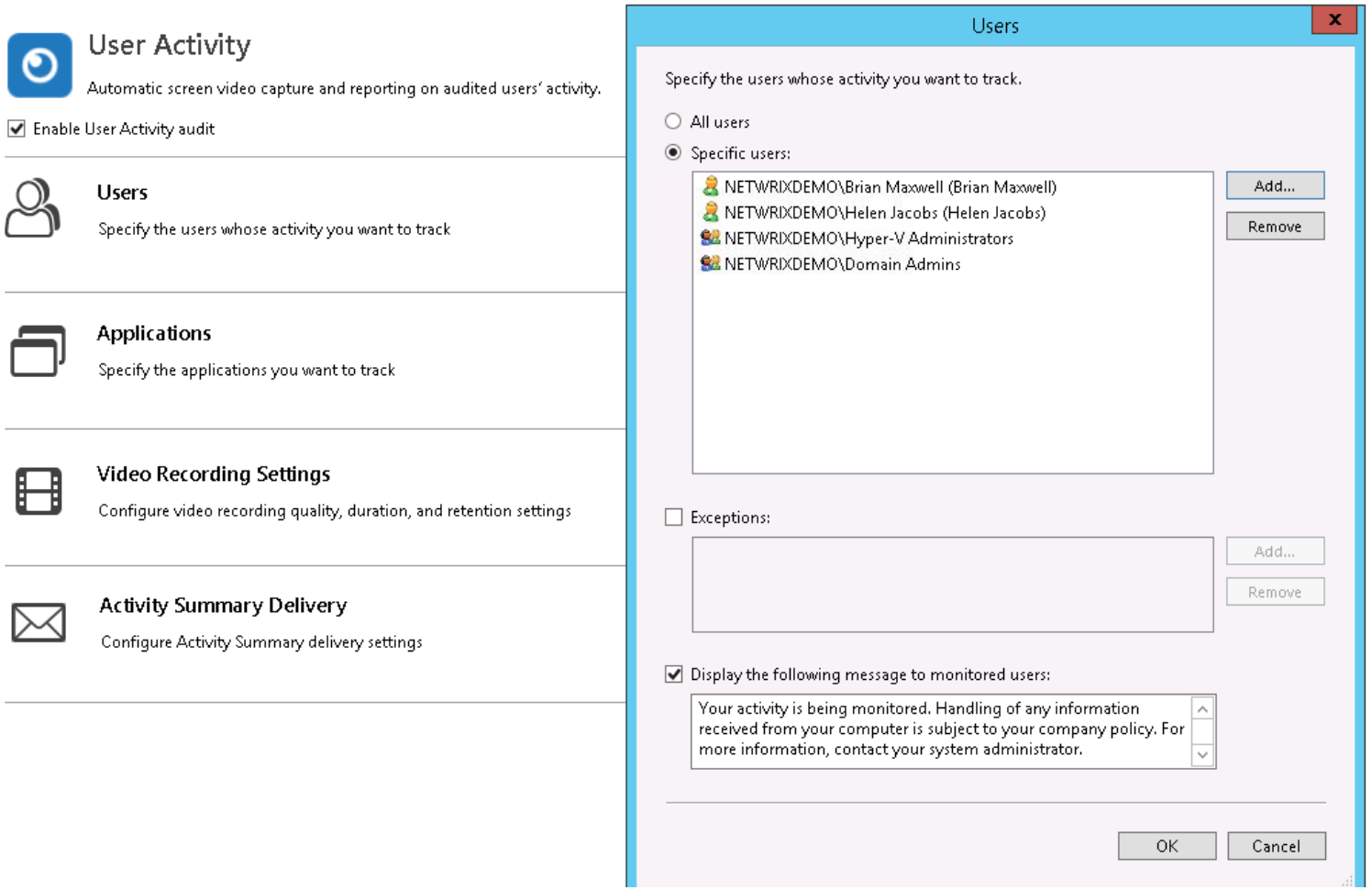
Shows all changes across the entire IT infrastructure grouped by the audited system.

Filter	Value

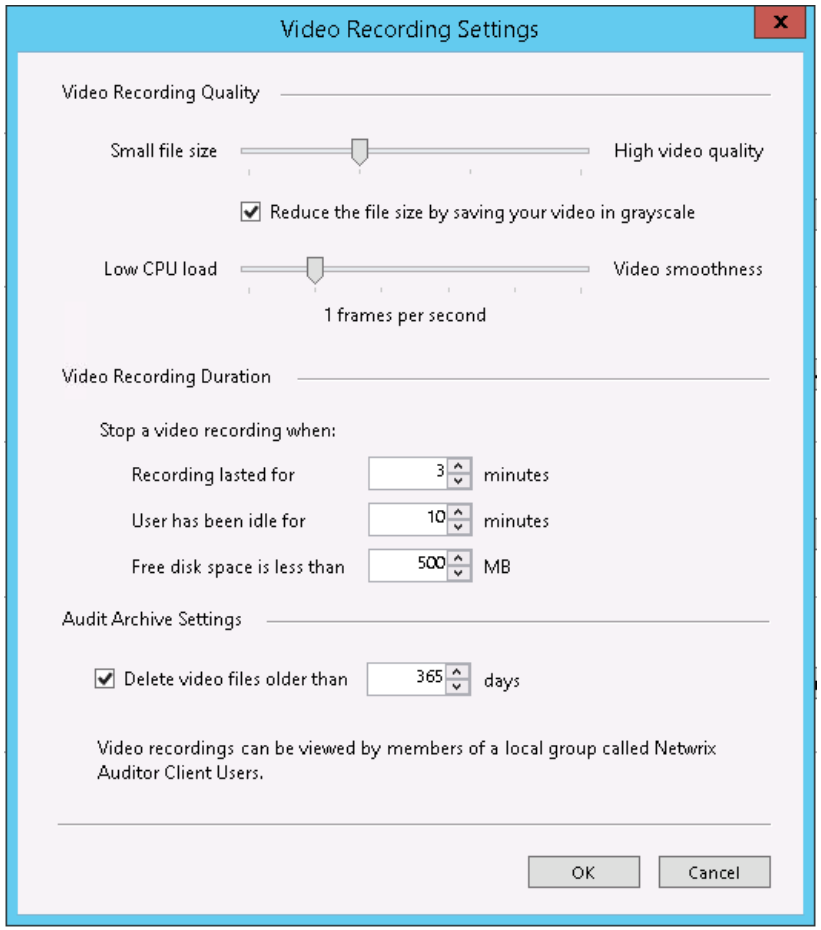
Audited System: Active Directory

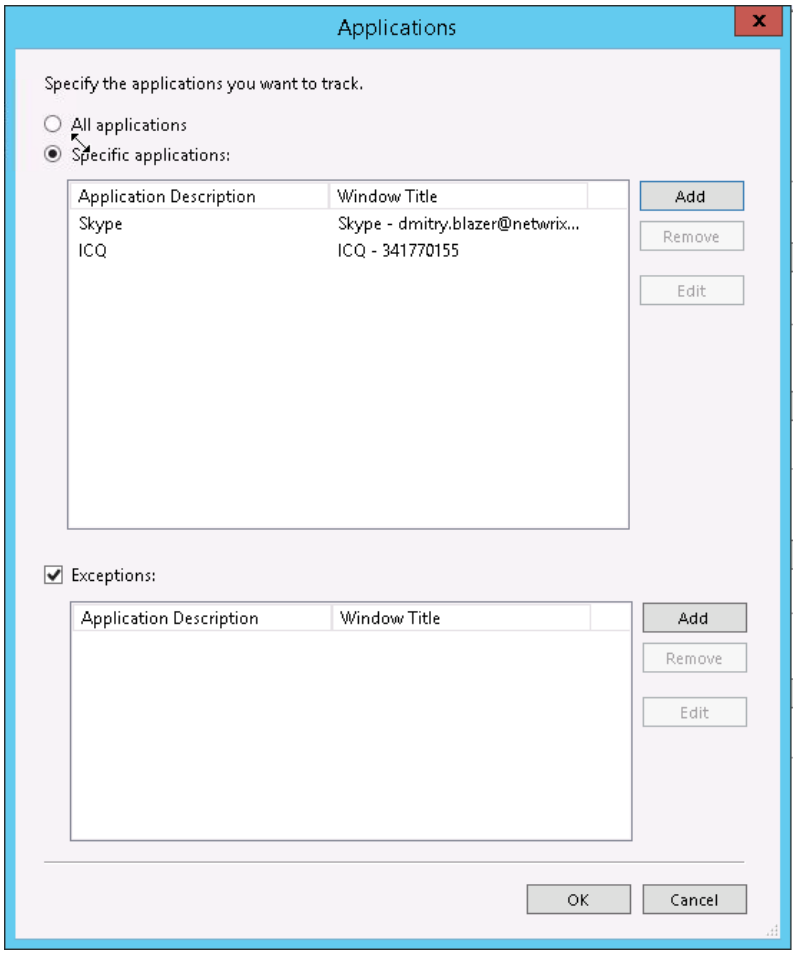
Action	Object Type	What Changed	Where Changed	Who Changed	When Changed
Added	User	\local\corp\Users\John Smith	rootdc1.corp.local	CORP\administrator	2/26/2014 5:17:56 AM
Added	User	\local\corp\Users\Brad Davis	rootdc1.corp.local	CORP\administrator	3/5/2014 4:55:26 AM
Added	User	\local\corp\Users\Greg Taylor	rootdc1.corp.local	CORP\administrator	3/6/2014 1:18:06 AM
Added	User	\local\corp\Users\Bob Brown	rootdc1.corp.local	CORP\administrator	3/6/2014 1:19:29 AM
Modified	Group	\local\corp\Users\Domain Admins	rootdc1.corp.local	CORP\administrator	3/19/2014 7:42:06 AM
Security Global Group Member added: "corp.local/Users/John Smith"					
Added	User	\local\corp\Users\Thomas Moore	rootdc1.corp.local	CORP\administrator	3/20/2014 1:50:06 AM
Added	Group	\local\corp\Users\Accountants	rootdc1.corp.local	CORP\administrator	3/20/2014 1:51:44 AM
Group Type "Security Domain Local Group"					
Members "\local\corp\Users\Thomas Moore"					
Added	User	\local\corp\Users\Anna Thompson	rootdc1.corp.local	CORP\administrator	3/20/2014 1:52:22 AM
Modified	Group	\local\corp\Users\Accountants	rootdc1.corp.local	CORP\administrator	3/20/2014 1:52:56 AM
Security Local Group Member added: "corp.local/Users/Anna Thompson"					
Added	User	\local\corp\Users\Sheila Hartford	rootdc1.corp.local	CORP\administrator	3/20/2014 1:53:57 AM

Видеозапись действий: выбор условий

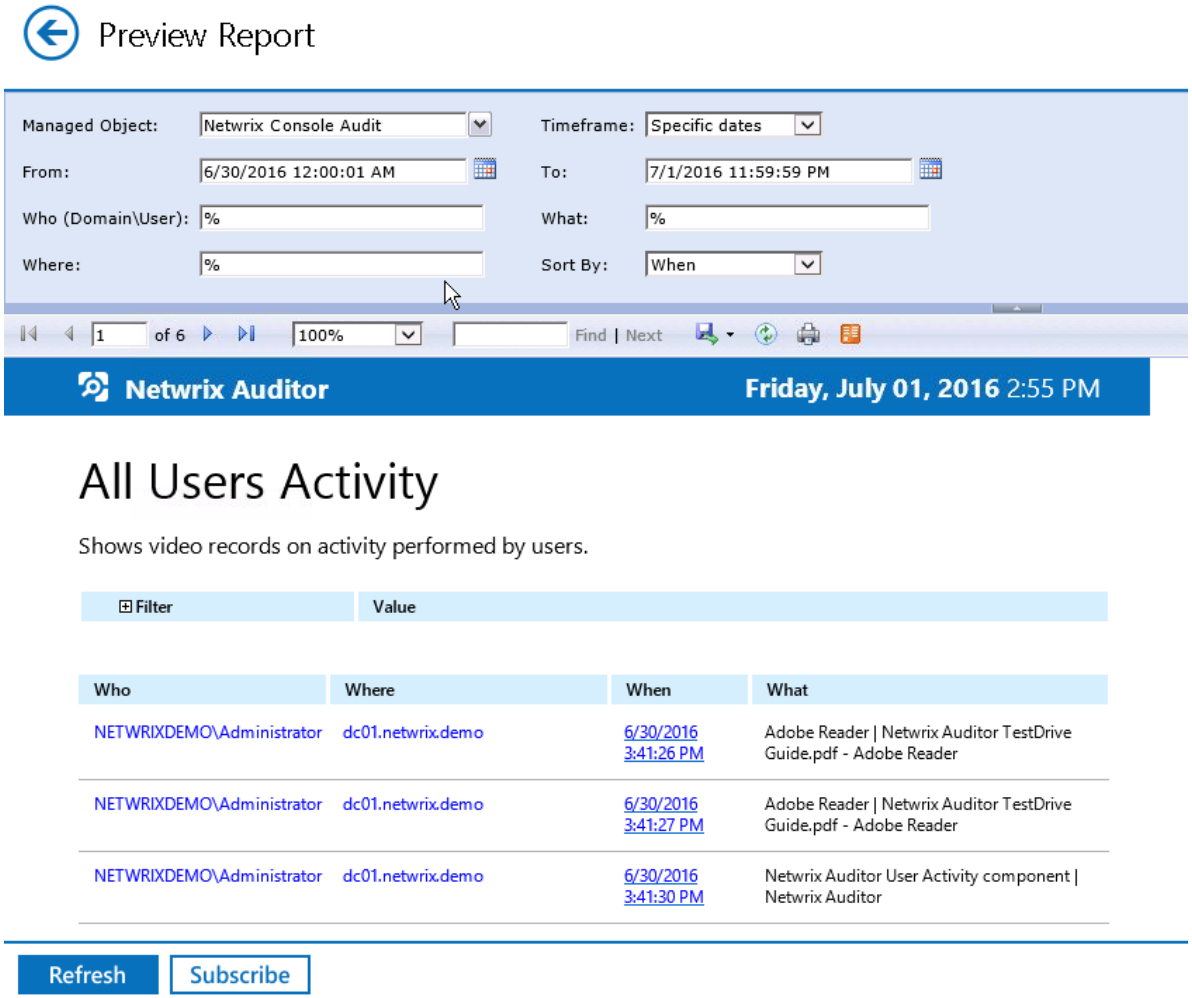


Видеозапись: настройки параметров

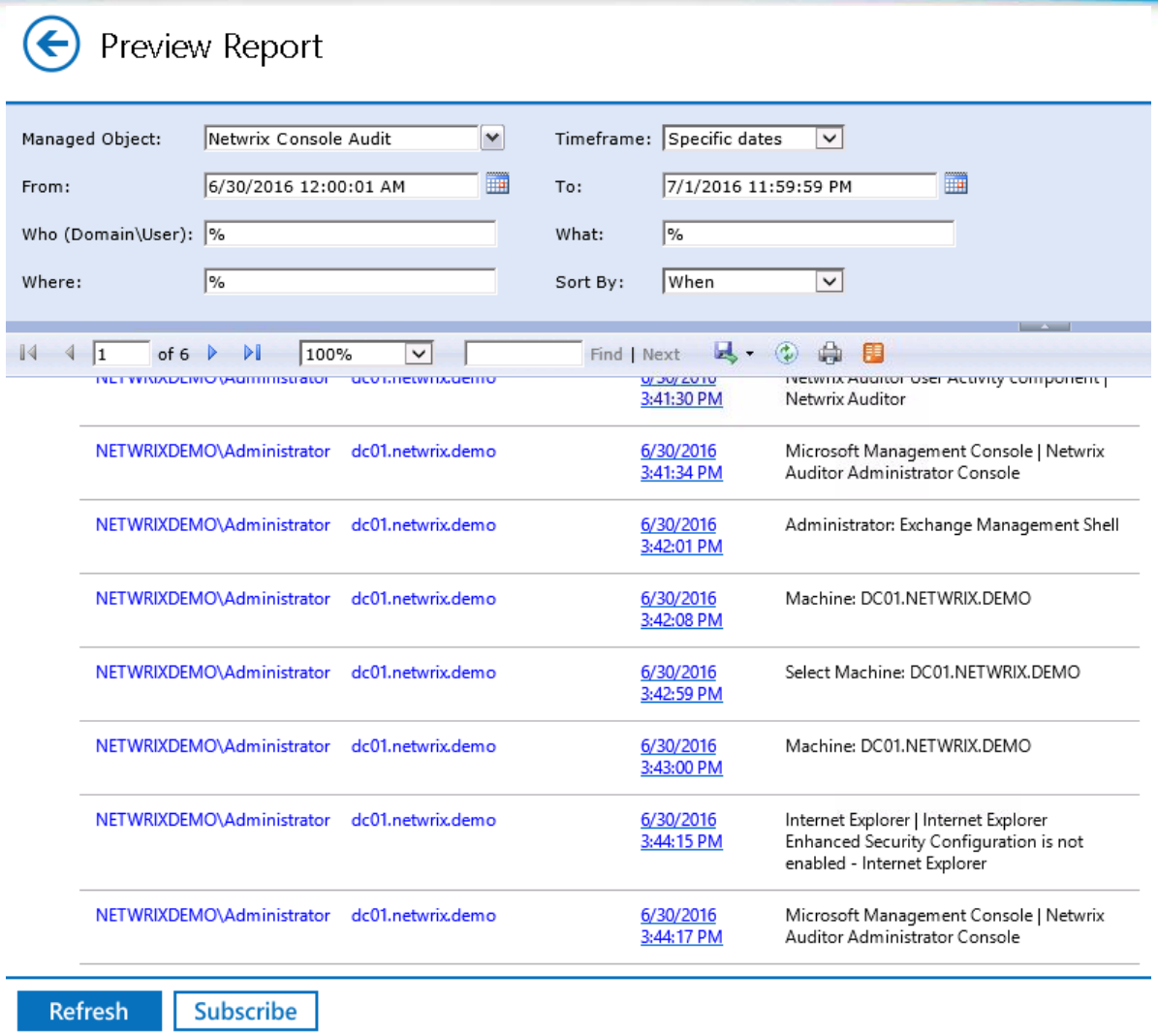




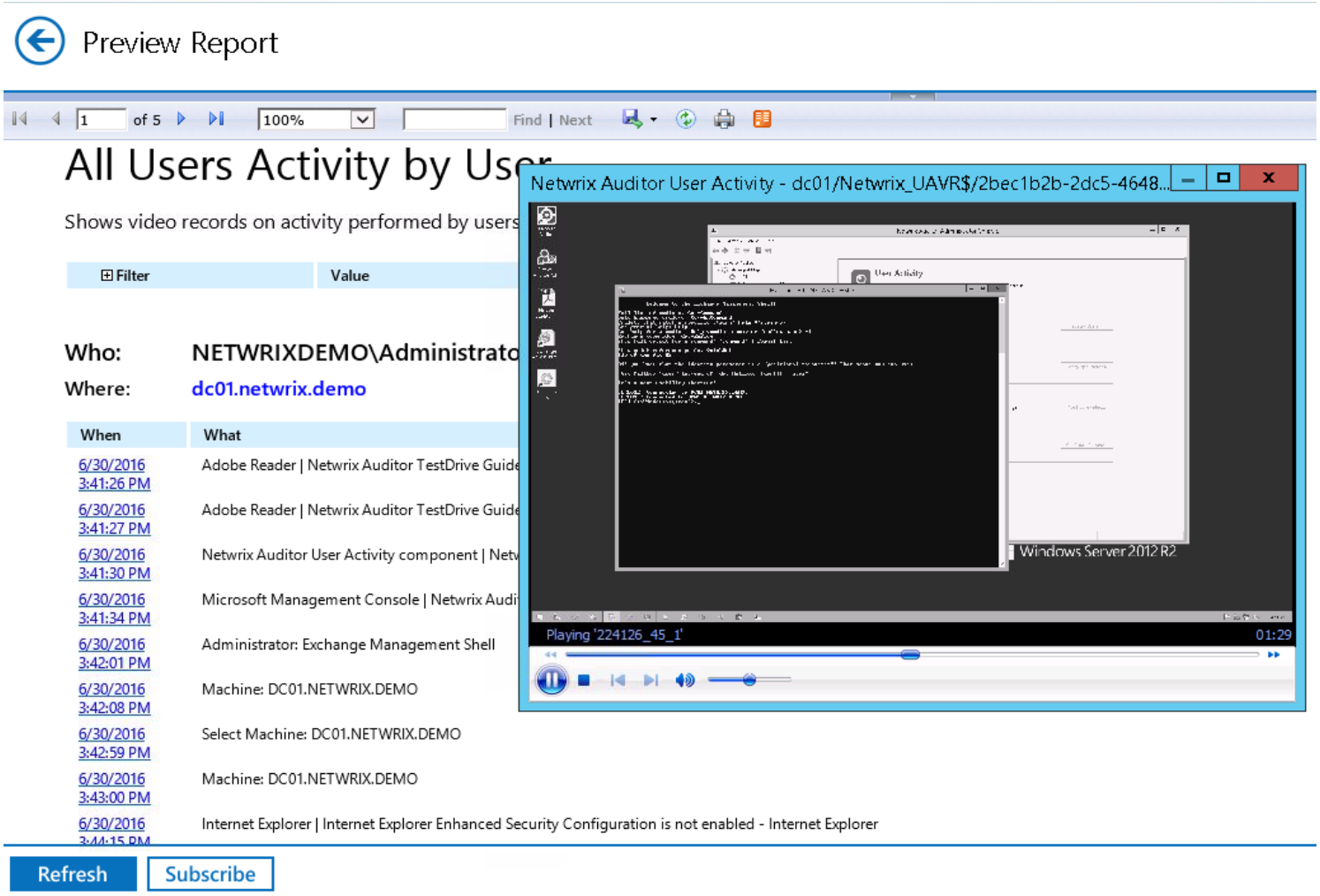
Видеозапись действий: отчет о действиях



Видеозапись действий: отчет о действиях



Просмотр действий пользователя



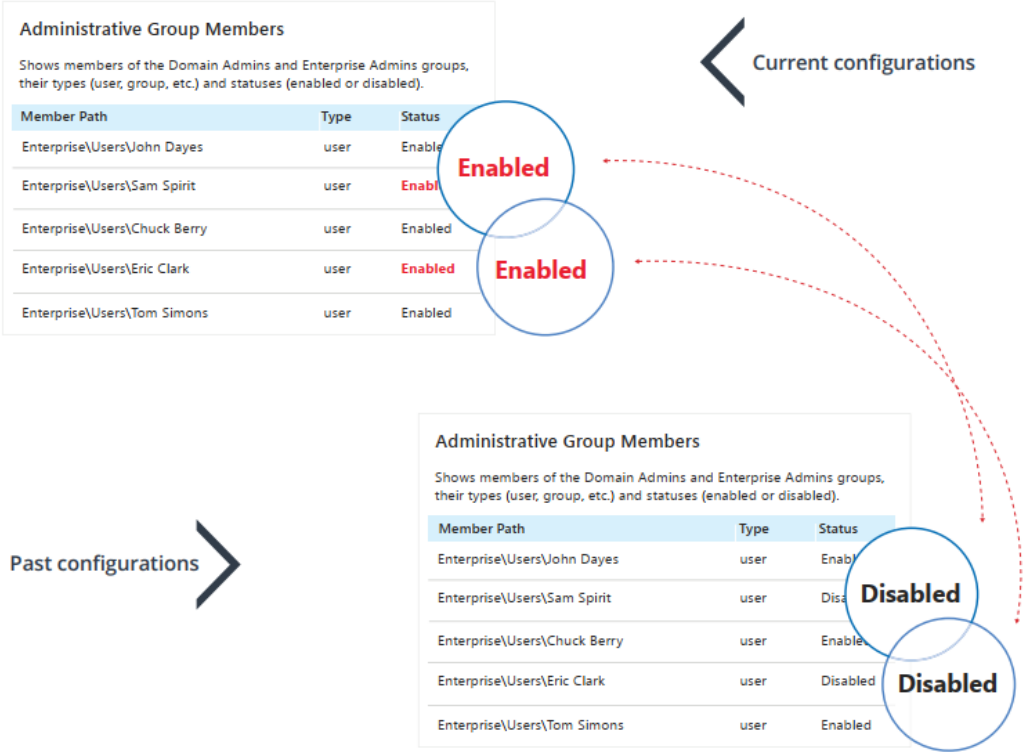
Дополнения Netwrix Auditor

1. Добавляют контекст в данные SIEM-систем
2. Помогают быстрее расследовать инциденты
3. Обеспечивают возврат инвестиций в SIEM

Дополнения Netwrix Auditor

4.1. Information about Group Policy attribute changes

Netwrix Auditor extends visibility into what's going on in your most critical IT systems by providing the state-in-time information for Active Directory and file server configurations. You can review configuration settings from any point in time — for example, you can see how group memberships or password policies were configured a year ago, and compare that to the current state. Easy access to this information help you ensure that business-critical IT systems are locked down, reducing risk.



Совместная работа

1. Пилотные проекты - бесплатно
2. Стенд в виртуальной среде «ТестДрайв»
3. Ключи на длительный период
4. Истории внедрения продуктов
5. Сравнения с конкурентами
6. Помощь в написании ТЗ
7. Документация для конкурсов

Чем отличаемся от остальных?

1. Компания выпускает один продукт, Netwrix Auditor.
   В течение 12 лет.

2. Продукт технически простой: постоянные усилия по настройке и сопровождение - не требуется

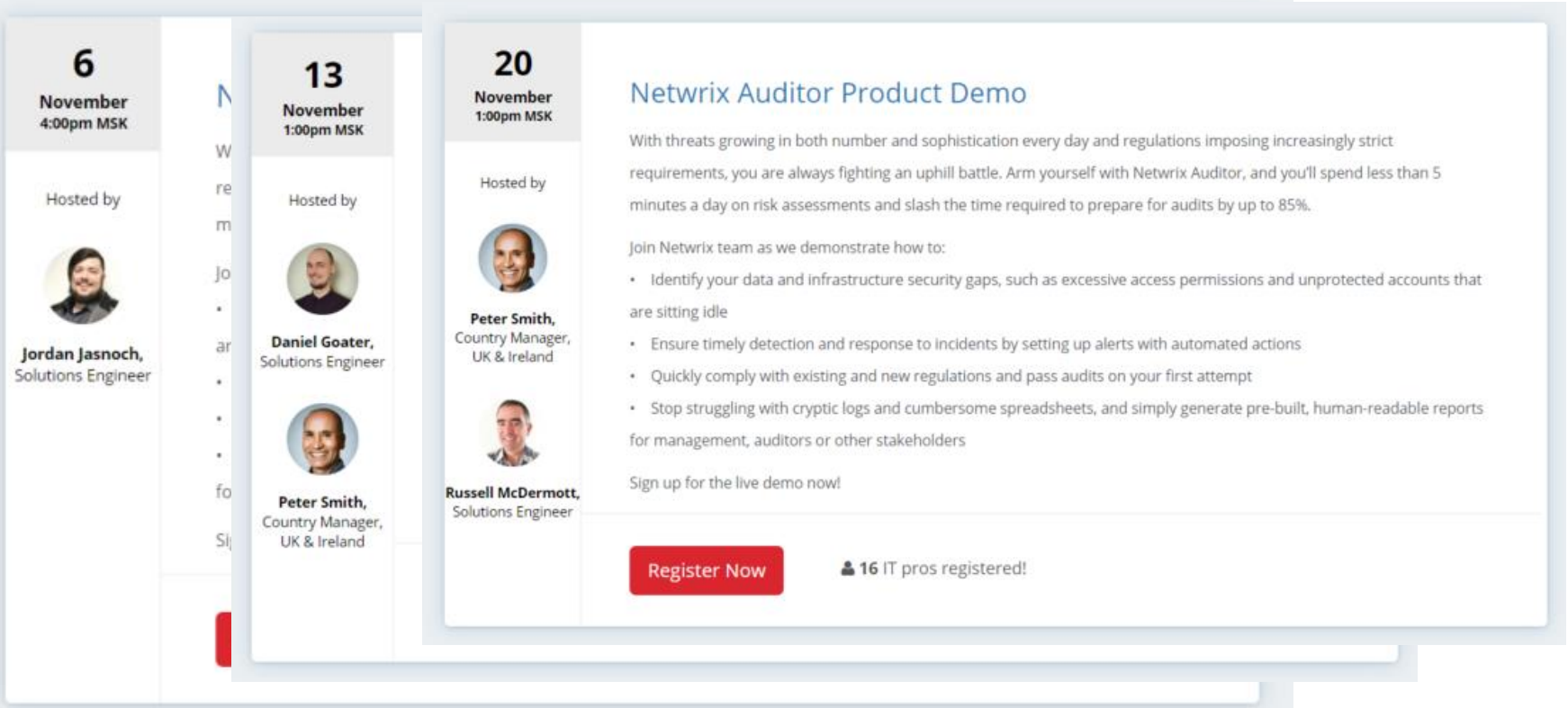
3. Проектирование, разработка, тестирование и поддержка
   в Санкт-Петербурге, на русском языке.

4. Быстрый доступ к инженерам производителя

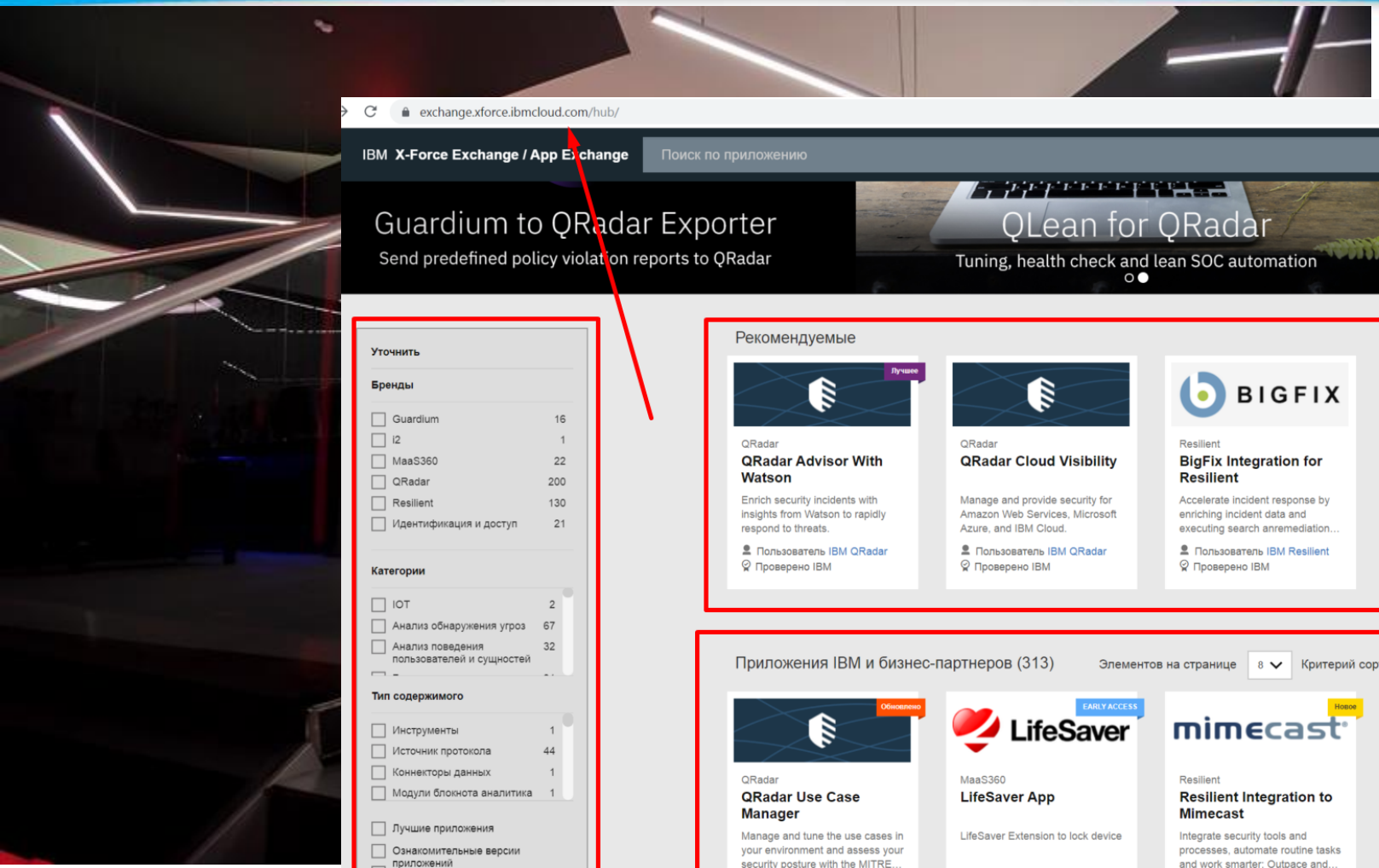
5. Netwrix Auditor - поддерживает все ключевые ИТ-системы

Будьте в курсе обновлений!

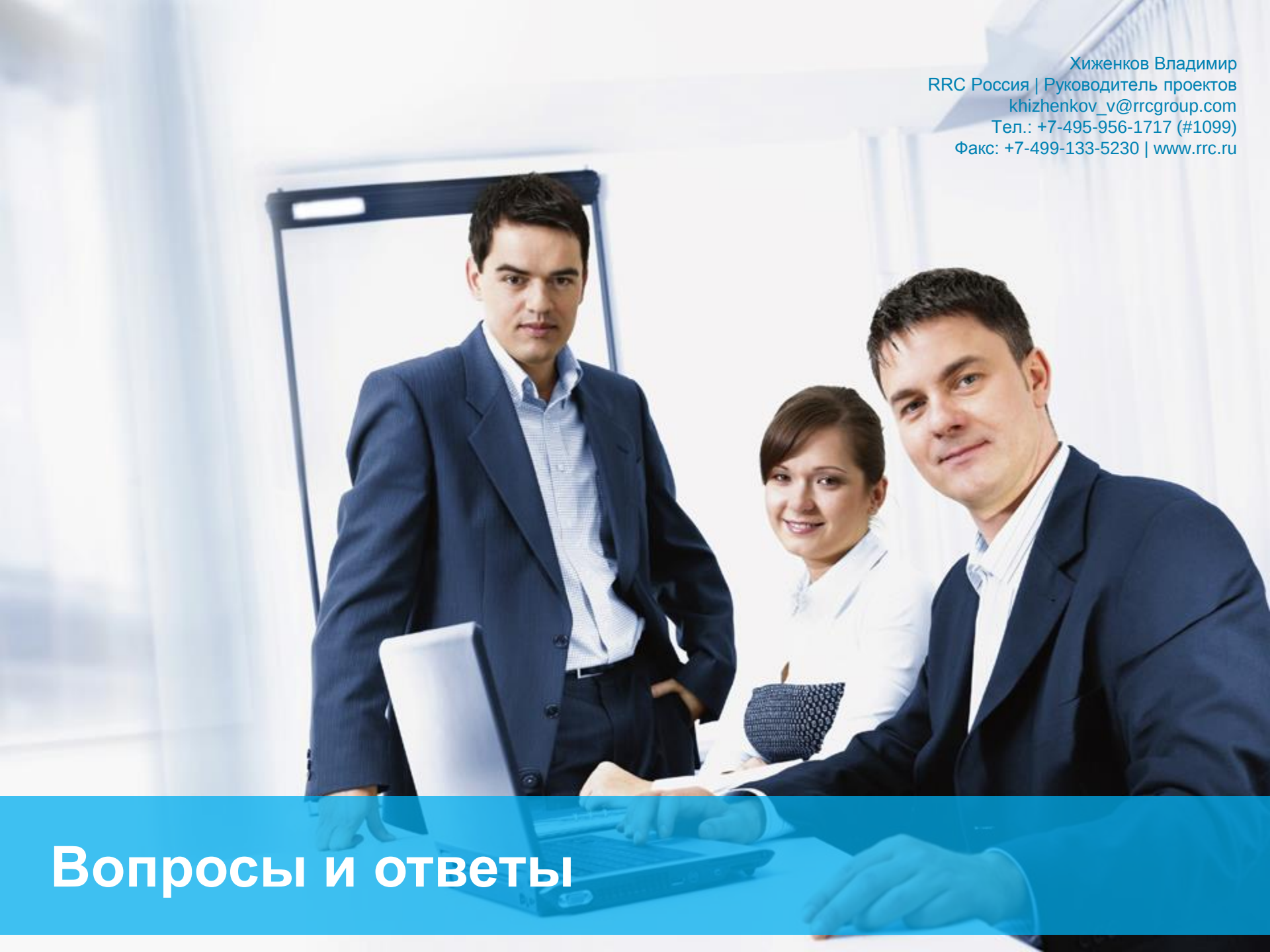
https://www.netwrix.com/webinars.html?_ga=2.2287280.1865628496.1572243889-1807408495.1572243889



Demo Room +QRadar solution



Хиженков Владимир
RRC Россия | Руководитель проектов
khizhenkov_v@rrcgroup.com
Тел.: +7-495-956-1717 (#1099)
Факс: +7-499-133-5230 | www.rrc.ru



Вопросы и ответы