netwrix

Netwrix Auditor

КОМПЛЕКСНОЕ РЕШЕНИЕ ДЛЯ АУДИТА ИТ-ИНФРАСТРУКТУРЫ
И УПРАВЛЕНИЯ ДОСТУПОМ К ДАННЫМ

netwrix.com/ru | netwrix.ru/social

01
Обзор продукта

Netwrix Auditor

Netwrix Auditor - это комплексное решение для эффективного контроля изменений в традиционных и облачных инфраструктурах. Netwrix Auditor позволяет предотвращать утечки данных, вызванные атаками инсайдеров, облегчает прохождение аудита на соответствие нормативам и позволяет быть в курсе изменений, которые вносят привилегированные пользователи в различные IT-системы.

Выявляйте подозрительную активность пользователей до того, как произойдет утечка данных.

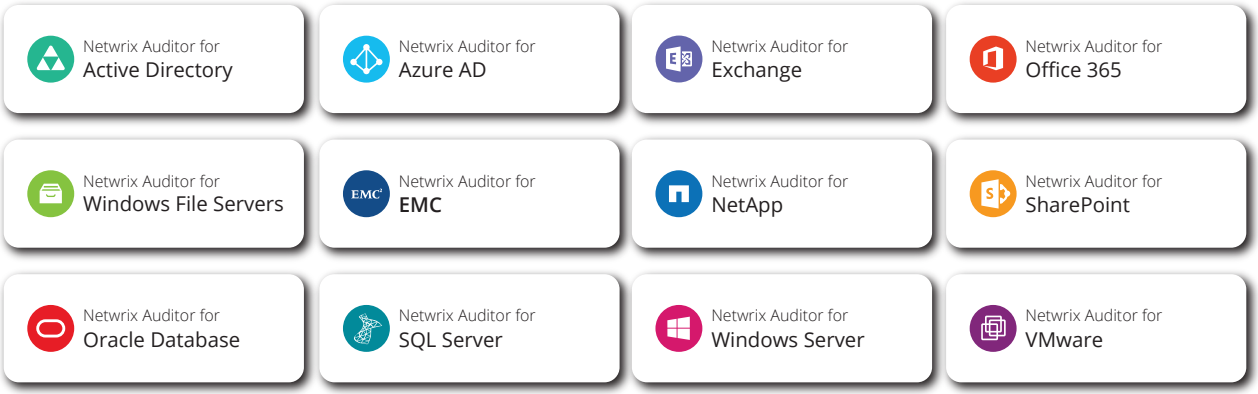
Проходите аудит на соответствие стандартам ИБ: PCI DSS,HIPAA, SOX, FISMA, ISO 27001 и другие.

Повышайте эффективность IT службы с помощью автоматического мониторинга и отчетности.

02 Приложения

Модули Netwrix Auditor

Netwrix Auditor **поддерживает широкий спектр IT систем**, включая Active Directory, Exchange, файловые серверы, SharePoint, SQL Server, VMware и Windows Server, Office 365, Azure AD, системы хранения данных EMC и NetApp, базы данных Oracle.



03 Преимущества

Усиление мер безопасности

Выявляйте потенциальные инсайдерские угрозы, контролируя изменения пользовательских данных, настроек различных систем, прав доступа, членства в группах и попытки получения доступа.

Расследуйте ИБ-инциденты и предотвращайте утечки данных, путем анализа изменений в настройках, отслеживания подозрительной активности и несанкционированного доступа к данным.

Преодолевайте ограничения встроенных средств аудита, уменьшая количество избыточных данных и получая контекст событий, используя технологию AuditAssurance™.

Соответствие нормативам

Убедитесь в том, что настройки ИТ-инфраструктуры соответствуют стандартам безопасности.

Используйте готовые отчеты, необходимые для прохождения аудита на соответствие нормативам PCI DSS, HIPAA, SOX, FISMA/ NIST800-53, COBIT, ISO/ IEC 27001 и др.

Храните данные о состоянии систем, правах доступа и всех изменениях в течение продолжительного времени - 10 лет и более. При необходимости, есть возможность обратиться к данным любого срока давности, для проведения аудита или расследования.

Оптимизация рабочих процессов

Сокращайте время подготовки отчетов: автоматическое формирование подробных и простых для восприятия отчетов сэкономит время сотрудников ИТ-службы, ускорит прохождение аудита на соответствие стандартам ИБ.

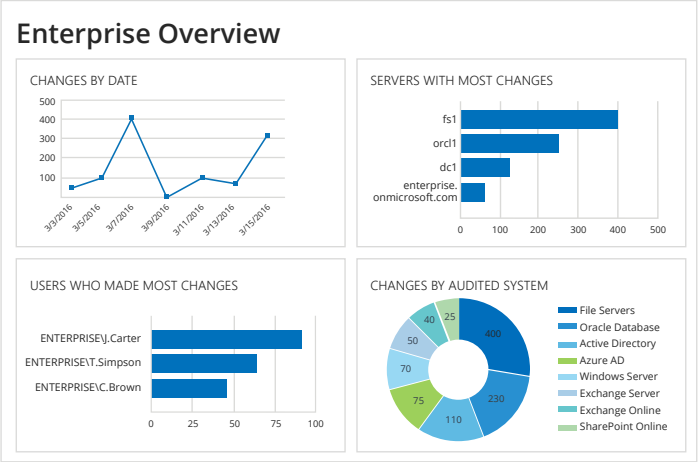
Предотвращайте простой системы и минимизируйте время устранения неполадок, вызванных ошибочными или некорректными изменениями в настройках приложений.

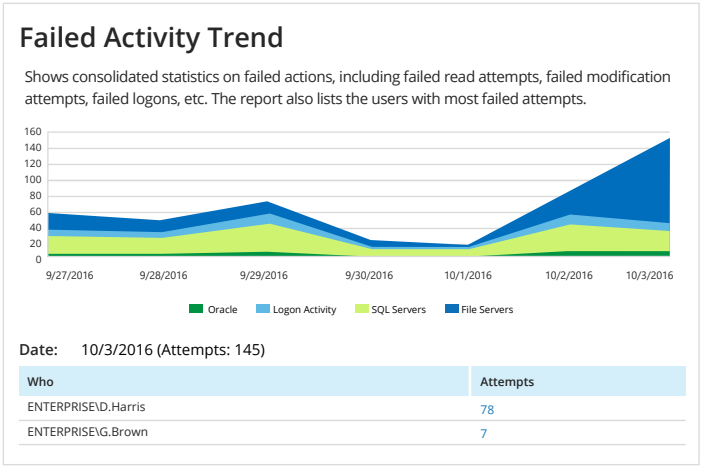
Проводите комплексный аудит ИТ-инфраструктуры **без лишних затрат**: ПО легко устанавливается и настраивается. Для работы с ПО не нужно проводить обучение специалистов.

04
Как это работает: Усиление мер безопасности

Полный контроль за событиями в ИТ-инфраструктуре

Получите общее представление о деятельности сотрудников в вашей ИТ-инфраструктуре, используя Enterprise Overview Dashboards. Обнаруживайте подозрительные действия сотрудников. Выясните, как часто производятся изменения, на какие системы они влияют и пр.





Обнаружение и анализ аномального поведения пользователей

Просматривайте статистику по таким инцидентам, как неудачная аутентификация в системе, неудачная попытка доступа к файлу (прочтение, изменение файлов).

05
Как это работает: Усиление мер безопасности

Контроль прав доступа и защита информации

Убедитесь в том, что только подходящие сотрудники имеют доступ к конфиденциальным данным. Для этого используйте отчет о действующих правах на файл или папку.

Object Permissions by Object

Shows accounts with their inherited or explicitly assigned basic permissions allowing them to access folders and subfolders, results are grouped by object path.

Folder path: \\fs1\Management\Finance

User Account	Permissions	User Permissions Inheritance
ENTERPRISE\Administrators	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Explicit
ENTERPRISE\J.Smith	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Inherited

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		
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			

Отслеживание доступа к неструктурированным данным

Используйте подписку на ежедневные отчеты, чтобы выявить тех, кто пытается получить доступ к важным файлам, например, номерам банковских карт, медицинским карточкам или банковским выпискам. Netwrix Auditor покажет, кто осуществлял попытки чтения или изменения файлов, на каком сервере и в какое время.

06
Как это работает: Усиление мер безопасности

Управление неструктурированными данными

Находите ненужные разрешения к данным, блокируйте неиспользуемые файлы, снижайте риск злоупотребления привилегиями.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks.

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

Action	Permissions	Means Granted	Times Accessed
ENTERPRISE\Administrator	Full Control	Group	258
ENTERPRISE\B.Atkins	Read (Execute, List folder content)	Group	14280
ENTERPRISE\H.Malicious	Read (Execute, List folder content)	Group	1745
ENTERPRISE\K.Smith	Read (Execute, List folder content)	Group	10020

Object: \\fs1\shared\Finance (Permissions: Same as parent)

Action	Permissions	Means Granted	Times Accessed
ENTERPRISE\B.Atkins	Modify (Read, Write, Execute)	Group	8680
ENTERPRISE\H.Malicious	Full Control	Directly	966

Changes to Admin Group Memberships

☑ Enable

Description:

Alert on changes to the Domain Admins and Enterprise Domain Admins groups

Edit...

Alert Filters

Specify filters for the changes that must trigger alerts:

- Addition to Enterprise Admins Group
- Removal from Enterprise Admins Group
- Addition to Domain Admins Group
- Removal from Domain Admins Group

Add... / Remove / Edit...

Notifications

Recipient	Type	Format
Administrator@enterprise.com	Email	Html

Add...

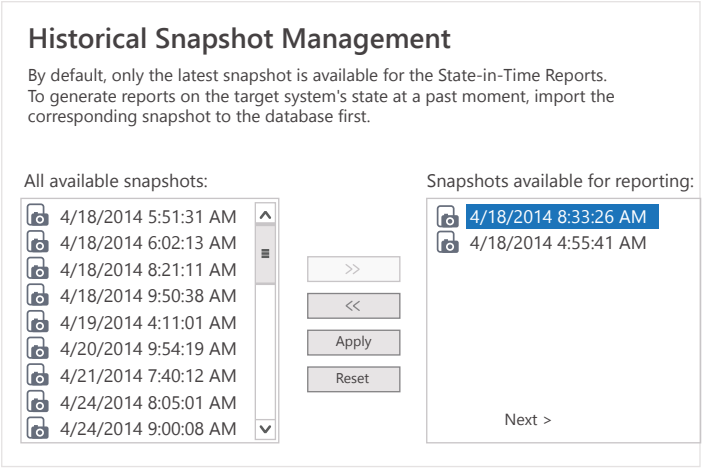
Оповещения при обнаружении подозрительных поведенческих паттернов

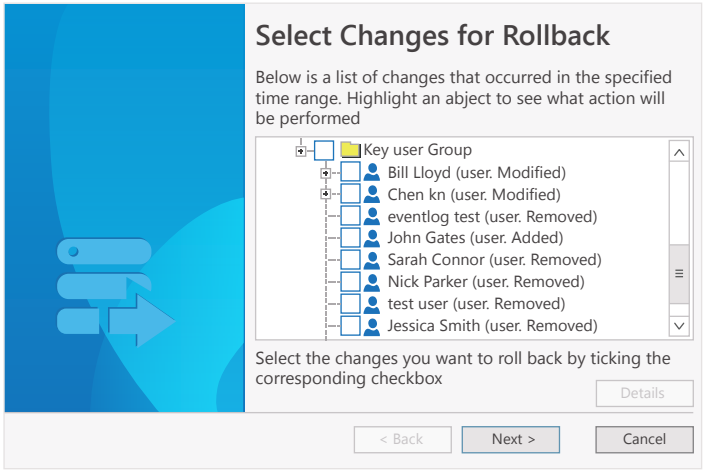
Отслеживайте подозрительные действия пользователей: добавление сторонних пользователей в группу Enterprise Admins, одновременный доступ к большому количеству файлов и т.д.

07
Как это работает: Усиление мер безопасности

Отображение настроек системы на любую заданную дату в прошедшем времени

Отчеты State-in-time™ показывают настройки различных систем на любую заданную дату в прошлом. Например, вы можете узнать, кто входил в определенную группу год назад, какой тогда была политика по настройке паролей. Такая информация может пригодиться для сравнения настроек с эталонными, а также при расследованиях инцидентов ИБ.





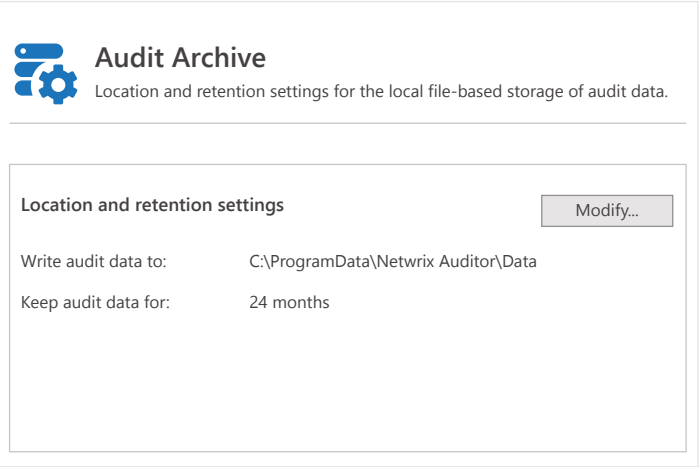
Восстановление объектов и их атрибутов

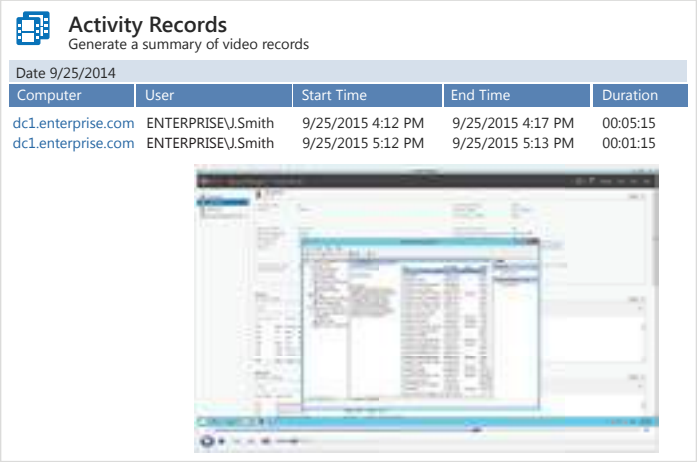
В случае, если в Active Directory произошли случайные или преднамеренные нежелательные изменения, вы можете вернуть все объекты AD и любые их свойства в предыдущее состояние, без перерывов в работе или длительных восстановлений из резервных копий.

08
Как это работает: Усиление мер безопасности

Долгосрочное хранение данных аудита

Двухуровневая система хранения данных аудита (БД SQL + файловый архив) AuditArchive™ позволяет обращаться к событиям, произошедшим 10 лет назад и более. Это может пригодиться для ретроспективного анализа при проведении расследований.





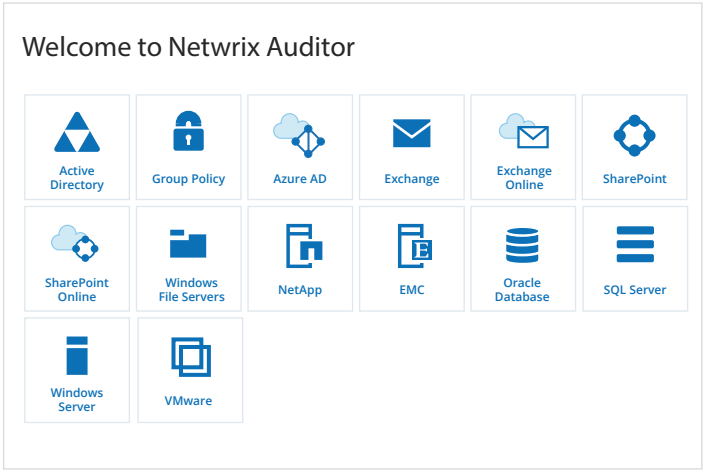
Контроль систем, не ведущих журналы событий

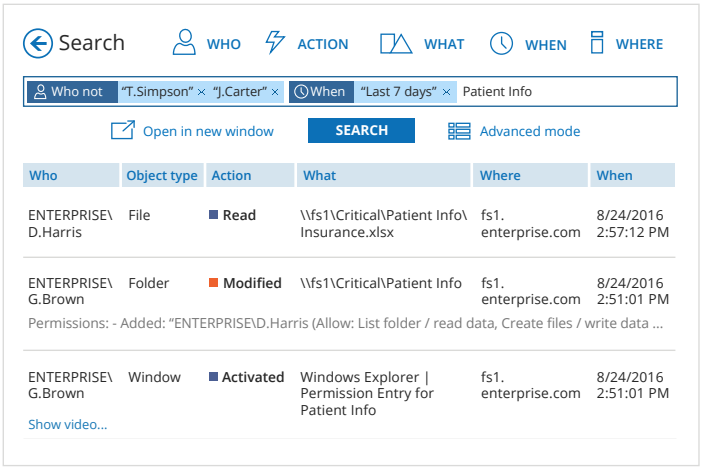
Вы можете контролировать изменения в системах, для которых не предусмотрено ведение журналов событий. Используйте видеозапись действий пользователей. Пишется не только происходящее на экране, но и метаданные: заголовки окон, процессы и пр., возможен поиск событий.

09
Как это работает: Соответствие нормативам

Отслеживание изменений в различных системах из единой консоли

Netwrix Auditor поддерживает основные системы, осуществляет их непрерывный мониторинг и собирает полученные данные в единые отчеты. Вы можете управлять событиями в различных приложениях из единой консоли.





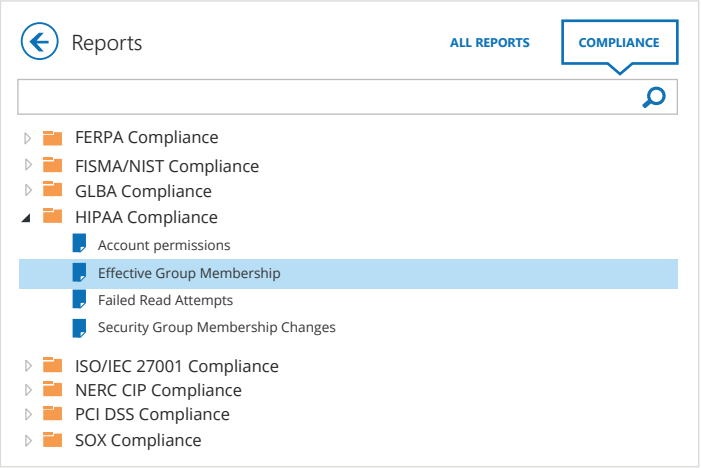
Оперативное предоставление информации проверяющим организациям

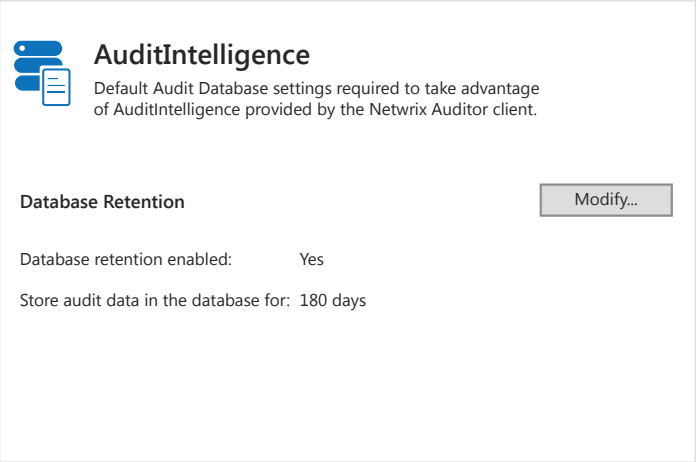
Вы можете предоставлять всю необходимую информацию проверяющим организациям быстрее, чем раньше. Например, вы можете быстро ответить на вопросы: «как изменялся состав группы Domain Admins год назад?» или «у каких пользователей были зафиксированы превышения полномочий?»

10
Как это работает: Соответствие нормативам

Шаблоны отчетов в соответствии с требованиями регуляторов

Используйте готовые отчеты, необходимые для прохождения аудита на соответствие нормативам PCI DSS, HIPAA, SOX, FISMA/ NIST800-53, COBIT, ISO/IEC 27001 и др.





Доступность данных аудита в течении 10 лет и более

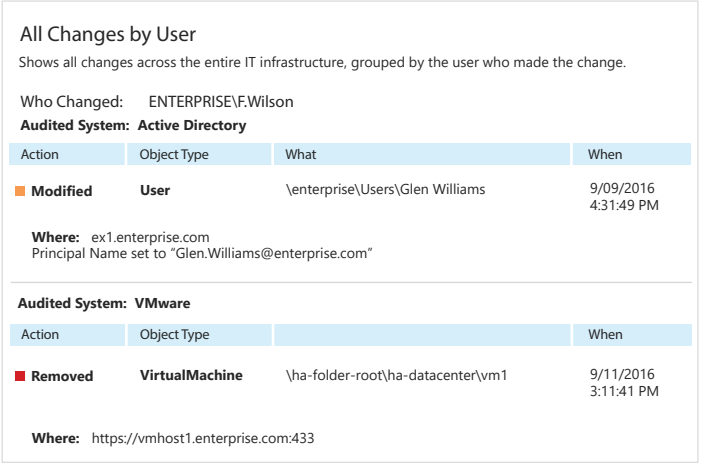
Собирайте данные о событиях с любого количества источников, преобразуйте их в простые, понятные отчеты. Система AuditIntelligence позволит хранить всю информацию в течении 10 лет и более, а также обеспечит легкий доступ к данным в любой момент.

11

Как это работает: Оптимизация рабочих процессов

Отслеживайте все изменения в ИТ-инфраструктуре

Получайте информацию о каждом изменении: что было изменено, где и кем, а также дату и время изменения, значения «до» и «после». Поддерживаются такие системы как: Active Directory, Групповые политики, серверы Microsoft Exchange, файловые серверы, среда Microsoft SharePoint, СУБД Microsoft SQL Server, виртуальная инфраструктура Vmware, а также машины под управлением ОС Windows.



All Changes by User

Shows all changes across the entire IT infrastructure, grouped by the user who made the change.

Who Changed: ENTERPRISE\F.Wilson

Audited System: Active Directory

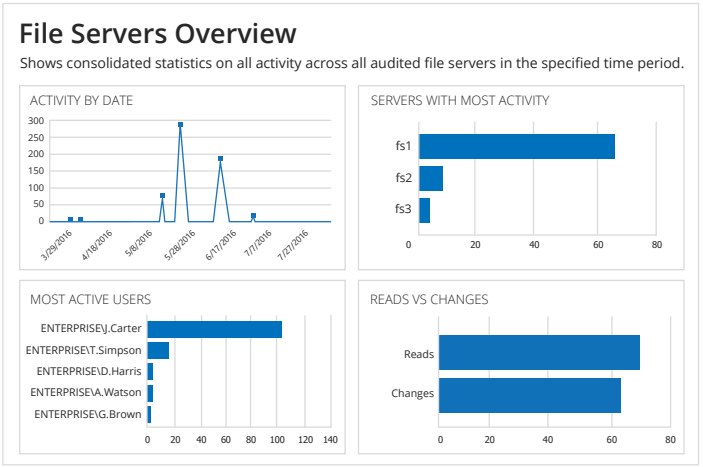
Action	Object Type	What	When
Modified	**User**	\enterprise\Users\Glen Williams	9/09/2016 4:31:49 PM

Where: ex1.enterprise.com
Principal Name set to "Glen.Williams@enterprise.com"

Audited System: VMware

Action	Object Type	What	When
Removed	**VirtualMachine**	\ha-folder-root\ha-datacenter\vm1	9/11/2016 3:11:41 PM

Where: https://vmhost1.enterprise.com:433



Простые и понятные отчеты

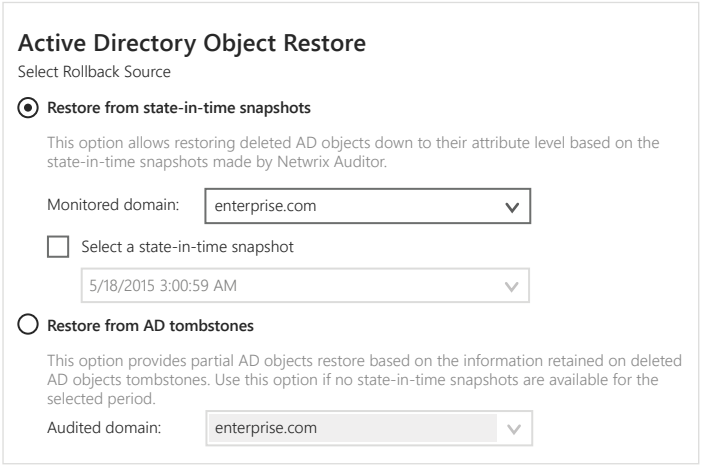
Просматривать бесконечные журналы событий или писать скрипты PowerShell больше не требуется. Библиотека Netwrix Auditor содержит более 150 готовых отчетов и графиков. В отчетах вы найдете всю необходимую информацию об изменениях в инфраструктуре, правах пользователей на любую дату, истекающих паролях и неактивных УЗ. Можно получать отчеты по почте, например, раз в неделю, настраивать фильтры, группировать и сортировать данные, а также экспортировать их в популярные форматы (PDF, XLS и др.).

12

Как это работает: Оптимизация рабочих процессов

Оперативное предоставление отчетов

Результаты запросов можно сохранять прямо на главной странице Netwrix Auditor для дальнейшего использования и предоставлять их коллегам. Это может сэкономить ваше время и значительно упростить совместную работу нескольких отделов вашей организации.



Предотвращение простоев системы

Если вы обнаружили в AD нежелательные изменения или узнали, что объекты AD были удалены, вы можете воспользоваться мастером восстановления объектов и вернуть ваш каталог в предыдущее состояние. Возврат изменений не требует простоев и перезагрузок, происходит за секунды – намного быстрее, чем при использовании средств резервного копирования.

13

Как это работает: Оптимизация рабочих процессов

Выборочная подписка на отчеты и оповещения

Вы можете получать оповещения об изменениях самых важных настроек в реальном времени. Например, вы получите оповещение в случае изменений в группах Enterprise Admins и Domain Admins.

Real-time Alert

Changes to Admin Group Membership

Severity	Critical
Domain	ENTERPRISE.COM
Change Type	Modified
Object Type	Group
When Changed	7/6/2015 4:58:53 AM
Who Changed	ENTERPRISE\J.Smith
Where Changed	dc1.enterprise.com
Object Name	\enterprise\Users\Domain Admins
Details	Security Global Group Member: • **Added:** "\enterprise\Users\Nick White"

All Group Policy Changes

Shows all changes to Group Policy objects, settings, links, and permissions, with the name of the originating workstation.

Action	What	Who	When
Modified	Security Policy	ENTERPRISE\J.Smith	9/23/2016 7:55:11 AM
Where:	dc1.enterprise.com		
Workstation:	172.17.35.12		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/ Account Policies/Password Policy		
Modified	Policy: Enforce password history; Setting: 24 passwords remembered -> 3 passwords remembered;		
Modified	Modified Policy: Maximum password age; Setting: 20 days -> 200 days;		
Modified	Modified Policy: Minimum password length; Setting: 7 characters-> 4 characters;		

Выявление действий злоумышленников

Отдельные события могут быть легитимными, но их последовательность позволяет говорить о действиях злоумышленника. Netwrix Auditor помогает выявить потенциальные утечки данных и причины внесения изменений в настройки ИТ-систем, поскольку собирает данные аудита комплексно.

14
Решение постоянных проблем ИТ-Департамента

System Administrator

Формируйте отчеты о соответствии нормативам быстрее.

Выявляйте подозрительные действия пользователей, предотвращая утечки данных.

IT Security Administrator

IT Manager

Контролируйте все события в IT-инфраструктуре и проходите аудит на соответствие нормативам.

Минимизируйте риски и затраты, связанные с соблюдением нормативов.

CIO/CISO

MSP

Обеспечьте полную прозрачность предоставляемых IT-инфраструктур.

15
Функции

Аудит изменений и контроль доступа

Аудит изменений: комплексный подход к отслеживанию изменений в ИТ-инфраструктуре. Формирование отчетов, содержащих информацию: кто, что, где и когда изменил. Отображение предыдущих параметров.

Аудит настроек: Отчеты State-in-time™ показывают настройки различных систем на любую заданную дату в прошлом. Например, вы можете узнать, кто входил в определенную группу год назад или какой тогда была политика по настройке паролей.

Контроль доступа: отслеживание удачных и неудачных попыток доступа к приложениям и данным.

Видеозапись действий пользователей на серверах и рабочих станциях во время интерактивных и удаленных сессий, отслеживание действий с критически важными приложениями, не осуществляющими запись в журналы событий.

Комплексное решение для аудита

Единое решения для аудита изменений: поддержка всех ключевых систем и приложений. Управление всеми событиями из единой консоли.

AuditAssurance™: автоматическая консолидация данных из множества независимых источников (журналы событий, снимки конфигурации (snapshots), записи об истории изменений), позволяет фиксировать изменения, даже если тот или иной источник не содержит всех необходимых данных.

AuditIntelligence™: трансформация большого количества данных аудита в простые и читаемые отчеты.

AuditArchive™: двухуровневая система хранения данных аудита (БД SQL + файловый архив) обеспечивает долгосрочное хранение информации и быстрый доступ к ней.

Доступ к данным на основе ролей: Система доступа к данным аудита позволяет разграничивать уровень доступа с учетом минимизации полномочий. Клиентская часть ПО Netwrix Auditor может использоваться на любом компьютере для получения отчетов и статистики.

Работа в режиме использования агентов и **без использования агентов.**

16
Функции

Отчеты и оповещения

Интерактивный поиск: позволяет задать вопрос на английском языке и быстро получить ответ – какие данные были изменены, кем и когда, а также - кто имеет или имел доступ к различным элементам ИТ-инфраструктуры.

Более 150 типов отчетов с возможностью фильтрации, группировки. Экспорт отчетов в различные форматы: Adobe Acrobat, PDF, MS Excel, MS Word, CSV. Веб-доступ к отчетам. Настройка расписания отправки отчетов.

Подготовка **матрицы прав доступа** для сертификации по ФЗ-152.

Шаблоны отчетов, сформированных по международным отраслевым стандартам: PCI DSS 3.0, HIPAA, SOX, FISMA/NIST800-53 и ISO/IEC 27001 и др.

Оповещения о всех типах событий в инфраструктуре в режиме реального времени.

Enterprise overview dashboards - наглядные графики изменений по всем контролируемым системам и приложениям. Возможность быстрого перехода от графиков к детальным табличным отчетам.

SIEM, возврат изменений

Интеграция с SIEM для оптимизации отчетности и сокращения ИТ-затрат. Поддержка RSA enVision®, ArcSight® Logger™, Novell® Sentinel™, NetIQ® Security Manager™, Symantec SIM IBM Tivoli® Security Information and Event Manager™.

Управление журналами событий: объединение, хранение журналов событий систем и устройств. Поддержка формата syslog, оповещения в реальном времени, веб-отчеты.

Возврат изменений: оперативное восстановление предыдущих настроек и свойств объектов, без перезагрузки системы и обращения к резервным копиям.

Варианты развертывания

Установите Netwrix Auditor в своей инфраструктуре,
в виртуальной среде или на облачной платформе

Традиционная инфраструктура	Виртуальные машины	Облачные платформы
Microsoft Windows Server	VMware	**Microsoft Azure**, AWS
	Microsoft Hyper-V	Amazon Web Services **Marketplace**
		CenturyLink Cloud Marketplace

Windows Server

Microsoft Hyper-V

vmware READY

Microsoft Azure

awsmarketplace

CenturyLink™

RESTful API — безграничные возможности мониторинга и отчетности, интеграция с любым установленным на сервере или в облаке приложением

Централизованный аудит и отчетность

Максимальная выгода от SIEM систем

Автоматизация IT процессов

Netwrix Auditor успешно интегрируется в инфраструктуру любого масштаба

ЛИНЗМАСТЕР САЛОНЫ ОПТИКИ

300 пользователей

Использование Netwrix Auditor для контроля изменений в Active Directory и групповых политиках.

аэроэкспресс

700 пользователей

Использование Netwrix Auditor для real-time мониторинга AD и сокращения времени реакции на инциденты.

ТрансКапитал Банк

2500 пользователей

Контроль действий привилегированных пользователей.

Транс Контейнер

5000 пользователей

Контроль изменений в Active Directory, групповых политиках и Microsoft Exchange.

Мнение Экспертов

Gartner

"...инструменты для аудита конфигураций позволяют проверить настройки ваших систем, привести их в соответствие с лучшими практиками и требованиями регуляторов..."

Redmond MAGAZINE

"...аудит инфраструктуры не самая простая задача, особенно если проводить его вручную. Обо всех мелких изменениях и деталях, которые раньше необходимо было запоминать, теперь заботится Netwrix Auditor..."

Windows IT Pro

".....победитель в номинациях «Лучший продукт для Active Directory/ Group Policy» и «Лучший продукт для Аудита и Соответствия стандартам» 4 года подряд... "

Petri IT Knowledgebase

"...решение получило 5 из 5 звезд и было рекомендовано для тестирования каждому заказчику, использующему AD..."

netwrix

Дополнительно

Пробная версия: скачайте бесплатную пробную версию ПО
netwrix.com/freetrial

Test Drive: тест-драйв ПО в виртуальной лаборатории Netwrix
netwrix.com/testdrive

One-to-One Demo: демонстрация ПО от инженеров Netwrix
netwrix.com/livedemo

Свяжитесь с отделом продаж для дополнительной информации
sales.russia@netwrix.com

НАГРАДЫ

ООО "Нетрикс Европа"
197374, Санкт-Петербург, Торфяная дорога, д. 7, лит. Ф

Телефон: +7 (812) 309-54-98
Email: sales.russia@netwrix.com

netwrix.ru/social