netwrix
#1 for change auditing

Netwrix Auditor

Обзор

Netwrix Auditor предлагает комплексный подход к отслеживанию изменений в IT- инфраструктуре для сокращения количества инцидентов ИБ, обеспечения непрерывности бизнес-процессов и соответствия отраслевым стандартам.

Netwrix Auditor контролирует все элементы инфраструктуры, отслеживая события и изменения настроек. Продукт постоянно взаимодействует с ключевыми информационными системами, выявляет, собирает и консолидирует данные. Архитектура Netwrix Auditor обеспечивает постоянную доступность информации для изучения истории модификаций инфраструктуры. В отличие от встроенных журналов событий, Netwrix Auditor применяет алгоритм компрессии данных для хранения информации. Такой подход позволяет быстро восстановить события любого срока давности, а также работать с большим объемом архивов без потери производительности. Хранение информации в течение нескольких лет является требованием многих стандартов: SOX и HIPAA – 7 лет, PCI DSS – 1 год.

Поддерживаемые платформы и приложения

- Active Directory
- Group Policy
- Exchange
- File Server
- VMware vSphere and ESX
- Windows event logs
- SQL Server
- SharePoint Server
- Windows Servers
- EMC
- NetApp
- Syslog

> “В решении Netwrix Auditor для Active Directory нас привлек тот факт, что ПО не устанавливает дополнительное программное обеспечение на контроллеры домена, полагаясь исключительно на штатные функции аудита. Недостающую информацию Netwrix Auditor получает посредством периодического создания снапшотов - моментальных снимков Active Directory.

Олег Ржевский,
Зам начальника Управления технической поддержки,
Транскапиталбанк

Награды

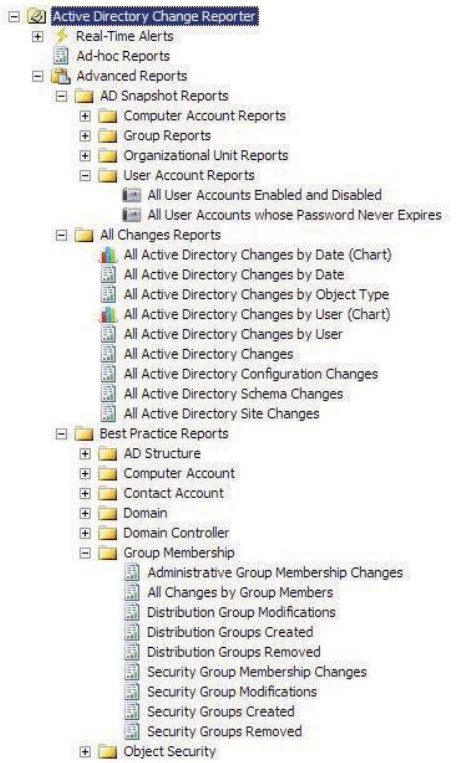
Более 50 наград: netwrix.com/ru/awards

Заказчики

Более 10,000 заказчиков: netwrix.com/ru/customers

Преимущества

- Оповещения о событиях в инфраструктуре в режиме реального времени
- Возможность восстановления предыдущих настроек и свойств объектов системы
- Детальные отчеты по заданным параметрам или из библиотеки стандартных отчетов (более 200 видов)
- Генерация матрицы прав доступа
- Отчеты, помогающие соответствовать международным и местным стандартам безопасности: SOX, HIPAA, FISMA, PCI и др.
- Долговременное хранение информации (до 7 лет и более)
- Возможность видеозаписи терминальных сессий, виртуальных рабочих столов Citrix, VMware или Microsoft (поддержка протоколов RDP, PCoIP и др.)
- Интеграция в инфраструктуру любого масштаба (1000 DC с 1 млн. пользователей и более)
- Поддержка SIEM-систем
- Использование технологии быстрого сбора данных AuditAssurance™, инновационный подход к хранению данных
- Поддержка на русском языке
- Единая консоль управления, удобный интерфейс



The following changes were detected in your Active Directory.
To rollback unwanted AD changes you may use **Netwrix Active Directory Object Restore.**

Change Type	Object Type	When Changed	Who Changed	Where Changed	Object Name	Details
Added	group	8/2/2012 8:35:16 AM	CORP\ administrator	rootdc1. corp.local	\local\corp\R&D	**Group Type** set to "Security Domain Local Group" **Members** set to "\local\corp\ Users\John Smith"
Modified	group	8/2/2012 8:35:40 AM	CORP\ PJohnson	rootdc1. corp.local	\local\corp\R&D	**Security Local Group Member:** Added: "corp.local/Users/John Smith"
Added	user	8/1/2012 6:52:45 AM	CORP\ administrator	rootdc1. corp.local	\local\corp\ Users\Bob Brown	none
Modified	group	8/1/2012 6:56:13 AM	CORP\ JGreen	rootdc1. corp.local	\local\corp\ Users\ Domain Admins	**Security Global Group Member:** Added: "corp.local/Users/Greg Taylor"
Added	user	8/1/2012 6:53:20 AM	CORP\ MPeterson	rootdc1. corp.local	\local\corp\ Users\Greg Taylor	none
Added	user	8/1/2012 6:50:57 AM	CORP\ administrator	rootdc1. corp.local	\local\corp\ Users\John Smith	none

Функции

Active Directory	Автоматическое отслеживание, оповещение и формирование отчетов об изменениях всех атрибутов всех объектов AD, добавленных, удаленных и измененных объектах AD. Фиксация значений до и после изменений. Восстановление первоначальных значений атрибутов и удаленных объектов.
EMC Storage	Аудит доступа к файлам и папкам, мониторинг систем хранения EMC VNX/VNXe/Celerra.
Generic Event Logs	Объединение, хранение журналов событий систем и устройств. Поддержка формата syslog, оповещения в реальном времени, веб-отчеты.
MS Exchange	Контроль изменений в настройках конфигурации, создаваемых и удаляемых почтовых ящиков, хранилищ [information stores], параметров протоколов и прав доступа. Фиксация значений до и после изменений.
File Server	Оповещения и отчеты об изменениях файлов и попытках доступа к файловым ресурсам. Подготовка матрицы прав доступа для сертификации по ФЗ-152, соответствия стандартам: Sarbanes-Oxley, HIPAA, PCI DSS и пр. Долгосрочное хранение данных аудита.
Групповые политики	Аудит изменений групповых политик: созданные и удаленные объекты групповой политики (GPO), изменения связей GPO, политик аудита и паролей, развертывания ПО, изменение конфигурации рабочих станций. Фиксация настроек политики до и после изменений.
NetApp Filer	Мониторинг систем хранения NetApp Filer, фиксация и оповещение о попытках доступа к файлам и их изменении.
SharePoint	Аудит административных настроек, изменений прав доступа и документов SharePoint
SQL Server	Контроль изменений в правах доступа к объектам SQL Server и аудит изменений содержимого таблиц. Учет изменений, которые внесли сторонние приложения, использующие SQL Server. Распознавание неавторизованных и нежелательных изменений.
Терминальные серверы, инфраструктура VDI	Эффективный видео мониторинг действий пользователей на терминальных серверах и рабочих станциях, сбор метаданных сессий для легкого поиска и фильтрации записей. Поддержка Citrix, PCoIP, RDP. Интеграция с отчетами других модулей Netwrix.

Виртуальная среда VMware	Аудит изменений виртуальной среды VMware: контроль создания виртуальных машин для предотвращения бесконтрольного роста их количества. Поддержка платформ VMware VI3 и выше, vSphere, ESX, ESXi.
Компьютеры под управлением ОС Windows	Автоматизированный контроль серверов под управлением ОС Windows, формирование отчетов по всем изменениям в конфигурации сервера: в аппаратных устройствах, драйверах, ПО, службах, сетевых настройках, правах доступа.
Microsoft SCVMM	Аудит изменений виртуальной среды Microsoft: аудит создания виртуальных машин для предотвращения бесконтрольного роста их количества, отслеживание избыточной загрузки ресурсов.
События входа в систему	Мониторинг всех событий входа пользователей в систему, контроль активности пользователей, составление отчетов. Долгосрочное хранение данных аудита.
Сетевые устройства	Автоматическое обнаружение сетевых устройств в заданном диапазоне IP-адресов. Аудит устройств и их параметров: интерфейс, порты, IP устройства, MAC-адреса, поддержка формата Syslog.
Прочие элементы	Напоминание об истечении срока действия и необходимости смены пароля и автоматическое отслеживание неактивных учетных записей

“Благодаря внедрению Netwrix Auditor у нас появилась возможность администрирования практически всех компонентов ИТ-инфраструктуры из одной консоли. С первых дней внедрения ПО были выявлены проблемы различного масштаба, которые были своевременно устранены. Это привело к повышению надежности и защищенности Active Directory и инфраструктуры компании в целом.

Илья Старков,
ИТ-менеджер,
Каспийский Трубопроводный Консорциум

“Netwrix Auditor удобен и понятен, прост в установке и настройке. Приятным дополнением является возможность использования бесплатной редакции сервера Microsoft SQL Express. Кроме того, производитель предоставляет квалифицированную техническую поддержку даже на этапе предварительного тестирования решения.

Роман Ламонов
Системный администратор,
Линзмастер

О Netwrix Corporation

Netwrix Corporation – международная компания, основанная в 2006 году, специализирующаяся на разработке, внедрении и сопровождении программного обеспечения для эффективного управления IT-ресурсами. Компания Netwrix предлагает инновационные технологии и приложения, неоднократно отмечаемые наградами на престижных международных конкурсах и IT-выставках. Netwrix помогает решать проблемы контроля и безопасности IT-инфраструктуры с помощью простых, надежных и эффективных продуктов, не требующих больших временных затрат на внедрение и настройку и не оказывающих негативного воздействия на существующую IT-систему. Офисы компании открыты в США, Великобритании и России

Netwrix Corporation
7Ф Торфяная дор., С-Петербург, 197374

Офисы:
New York, Atlanta, Columbus, London

Тел: +7 (812) 309-5498
Int'l: +1 (949) 407-5125
EMEA: +44 (0) 203-318-0261