netwrix

Netwrix Auditor

Выявляйте угрозы безопасности, подтверждайте соответствие нормативным требованиям и повышайте эффективность работы ИТ-отдела

www.netwrix.ru

01
Product Overview

IT-аудит без проблем

Внутренний и внешний ИТ-аудит становится неотъемлемой частью повседневной жизни все большего числа организаций. Это естественно: ИТ-аудит не только играет ключевую роль в обеспечении безопасности и соблюдении требований законодательства, но и помогает организациям повышать эффективность рабочих процессов. К сожалению, регулярное проведение аудита отнимает гораздо больше сил и времени, чем следует.

Решения Netwrix Auditor упрощают прохождение аудита и помогают достичь поставленных целей с меньшими усилиями. Готовые настройки анализа позволяют автоматизировать значительную часть задач по обеспечению безопасности и соответствия нормативным требованиям, а также повседневной работы ИТ-отдела. Освободившееся время вы можете потратить на решение других задач, стоящих перед организацией, без постоянных переработок.

> *«Мы предпочитаем не поставщиков, а партнеров. Netwrix практически стал частью нашей команды. Благодаря Netwrix Auditor ИТ-отдел экономит драгоценное время, и в результате повышается эффективность нашей работы на благо людей».*

Джон Адамс, ИТ-директор, округ Вашингтон, шт. Арка

02
Обзор решения

Выявляйте угрозы быстрее, чтобы не стать жертвой утечки данных

Снизьте риски для критически важных данных путем выявления основных проблем с их безопасностью и отключения чрезмерно широких прав доступа. Своевременно выявляйте угрозы и реагируйте на них благодаря настройке уведомлений с автоматическими действиями, а также более быстрому и точному расследованию ИБ-инцидентов.

Снижайте затраты времени и средств на прохождение аудита на соответствие стандартам

Обеспечивайте и подтверждайте соответствие нормативным требованиям с меньшими затратами сил и средств, сократите время, необходимое для подготовки к аудиту, на 85%. Не тратьте лишнее время на анализ журналов аудита, чтобы ответить на неожиданные вопросы проверяющих.

Повышайте эффективность работы ИТ-отдела без чрезмерного увеличения нагрузки на сотрудников

ИТ-отдел сможет делать больше при меньших затратах и добиваться высоких показателей без постоянных переработок. Устраняйте критически важные проблемы, прежде чем они помешают работе пользователей и компании, готовьте необходимую информацию для руководителей быстрее, чем раньше.

03

Быстрее выявляйте угрозы, чтобы не стать жертвой крупной утечки данных.

Оценивайте и снижайте ИТ-риски

Выявляйте и устраняйте проблемы с безопасностью данных и инфраструктуры, например, большое число непосредственно предоставленных прав доступа или чрезмерное количество неактивных учетных записей пользователей, чтобы снизить поверхность атаки.

Risk Assessment – Overview

Risk name	Current value	Risk level
Users and Computers		
User accounts with Password never expires	2	Medium (1-4)
User accounts with Password not required	0	Low (0)
Inactive user accounts	10% (3 of 30)	High (1% - 100%)
Inactive computer accounts	20% (4 of 20)	High (3% - 100%)
Permissions		
User accounts with administrative permissions	20% (6 of 30)	High (3% - 100%)
Empty security groups	6% (0 of 50)	Low (0)
Data		
Shared folders accessible by Everyone	11% (1685 of 15321)	Medium (5% - 15%)
File names containing sensitive data	2	High (2 - unlimited)
Potentially harmful files on file shares	0	Low (0)
Direct permissions on files and folders	21% (10759 of 51237)	High (5% - 100%)

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.

Content source	Categories	Files count
\\fs1\Accounting	GDPR	1300
	PCI DSS	585
\\fs1\Finance	GDPR	715
	HIPAA	1085
	PCI DSS	952
\\fs1\HR	GDPR	1500
	HIPAA	250
\\fs1\Public	PCI DSS	15

Проводите глубокий анализ конфиденциальных данных

Определяйте местоположение и классифицируйте конфиденциальную информацию SharePoint, в том числе данные банковских карт, медицинские записи и другие персональные данные. Выявляйте данные, которые находятся в незащищенных хранилищах, чтобы минимизировать риск утечки.

04

Быстрее выявляйте угрозы, чтобы не стать жертвой крупной утечки данных.

Упростите регулярное подтверждение прав доступа

Анализируйте права доступа к различным конфиденциальным данным и пути получения этого доступа; предоставляйте владельцам данных возможность регулярно проверять соответствие прав доступа согласно служебной необходимости.

Sensitive Data Object Permissions

For each SharePoint object (site, list or document) listed, this report shows the user accounts that have access to this object, their effective permissions and how those permissions were granted. Use this report to control access to SharePoint objects that contain sensitive data.

Object path: http://sp.enterprise.com/sites/HR/Shared/Candidates Info 2019.xlsx

Categories: PII

Total accounts count: 5

User account	Permissions	Means granted
ENTERPRISE\J.Carter	Full Control	Zone: Default (policy), Web application pool account
ENTERPRISE\T.Simpson	Full Control	Zone: Default (policy), Web application pool account
ENTERPRISE\A.Brown	Full Control	Farm Account
ENTERPRISE\B.Richter	Read	Permission level, Site collection administrator
ENTERPRISE\J.London	Contribute	Farm Account

User Sessions

Use this report to identify suspicious user sessions on Windows servers. Find out which users were active on critical or terminal servers and the total time during a day when their activity on the servers was monitored by Netwrix Auditor.

When: 4/23/2019

Who: ENTERPRISE\J.Carter

Where	Active time
audit.enterprise.com	3:05
dc1.enterprise.com	0:14

Who: ENTERPRISE\T.Simpson

Where	Active time
audit.enterprise.com	0:09
dc1.enterprise.com	0:32

Устанавливайте строгий контроль использования привилегированных учетных записей

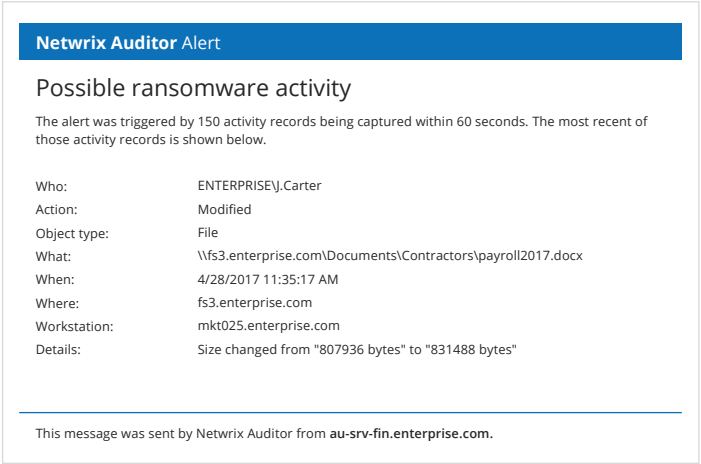
Ведите мониторинг активности администраторов и других привилегированных пользователей во всех системах, чтобы убедиться, что они соблюдают внутренние политики и не злоупотребляют полномочиями.

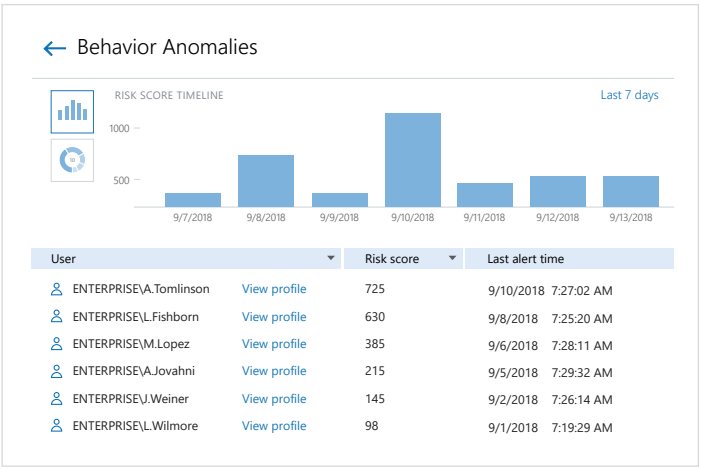
05

Быстрее выявляйте угрозы, чтобы не стать жертвой крупной утечки данных.

Узнавайте первыми о подозрительных действиях пользователей

Выявляйте угрозы безопасности, такие как использование сервера SQL в нерабочее время или большое число повторяющихся изменений файлов, которое может указывать на атаку программ-вымогателей, и принимайте меры, чтобы предотвратить значительный ущерб.





Выявляйте взломанные учетные записи и внутренних злоумышленников

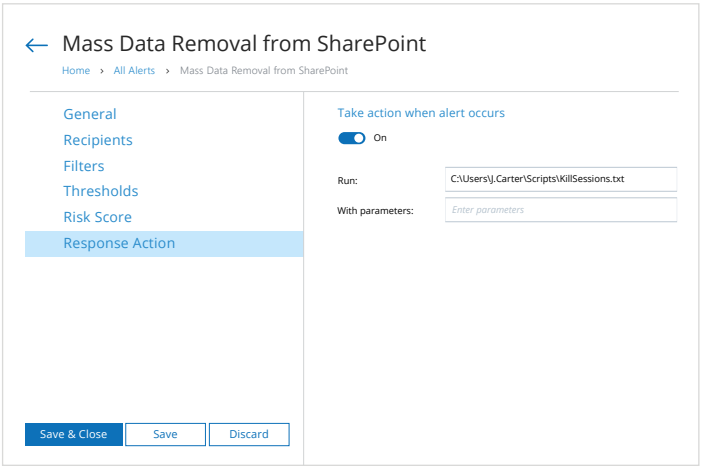
Находите даже незначительные признаки возможных угроз безопасности, таких как необычный вход в систему или несанкционированный удаленный доступ к сети. Определяйте пользователей, представляющих наибольшую опасность, и проводите расследование благодаря обзору подозрительной активности каждого пользователя.

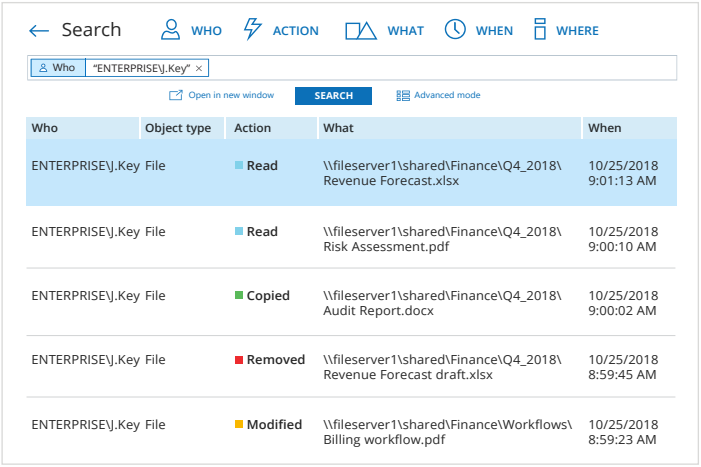
06

Быстрее выявляйте угрозы, чтобы не стать жертвой крупной утечки данных.

Сокращайте время реагирования на угрозы

Быстрее реагируйте на угрозы безопасности данных благодаря автоматизации действий при ожидаемых инцидентах. Обеспечивайте базовый уровень реагирования на ИБ-инциденты путем интеграции Netwrix Auditor в существующие процессы обеспечения безопасности.





Упрощайте расследование ИБ-инцидентов

Быстро устанавливайте причины инцидентов, затрагивающих конфиденциальные данные, используя Google-подобный поиск: точно выясняйте, что именно произошло, как это произошло, кто за этим стоял и какие блоки информации были затронуты.

07

Снижайте затраты времени и средств на прохождение аудита на соответствие стандартам

Обеспечивайте эффективность системы безопасности

Внедряйте контроль за соответствием нормативным требованиям для всей инфраструктуры и регулярно проверяйте его работу. Если задокументированные политики безопасности отличаются от реально используемых, необходимо немедленно исправить ситуацию, пока это не обнаружили аудиторы.

Sensitive File and Folder Permissions Details

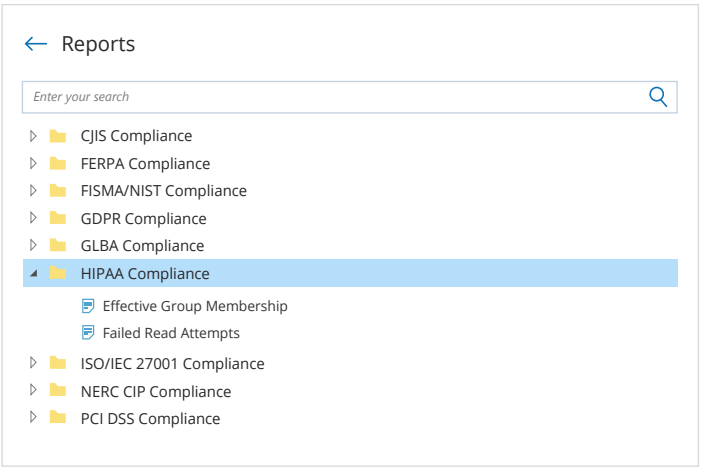
Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, via either group membership or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

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

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\Contractors (Permissions: Different from parent)
Categories: GDPR

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



Сокращайте время на подготовку и аудит соответствия нормативным требованиям

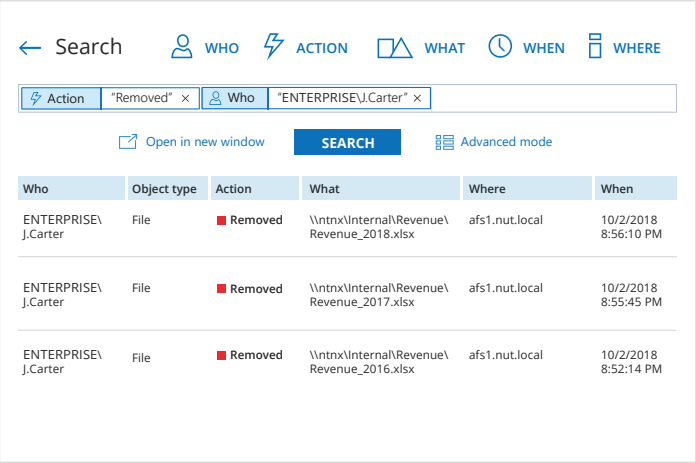
Быстрее подготовьте ответы на большинство вопросов аудиторов с помощью готовых отчетов, не требующих дополнительной настройки и соответствующих процедурам контроля соответствия требованиям HIPAA/HITECH, PCI DSS, GDPR и других современных стандартов.

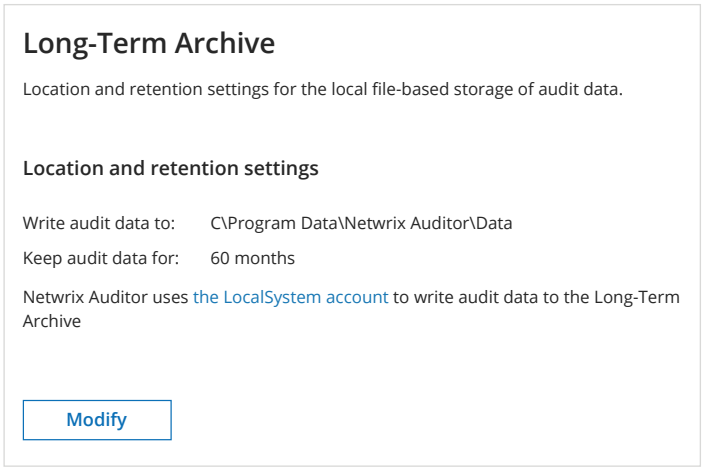
08

Снижайте затраты времени и средств на прохождение аудита на соответствие стандартам

Отвечайте на неожиданные вопросы аудиторов

При возникновении неожиданных вопросов в ходе аудита используйте функцию Google-подобного поиска для быстрого извлечения необходимой информации.





Храните контрольные журналы в удобном месте в течение многих лет

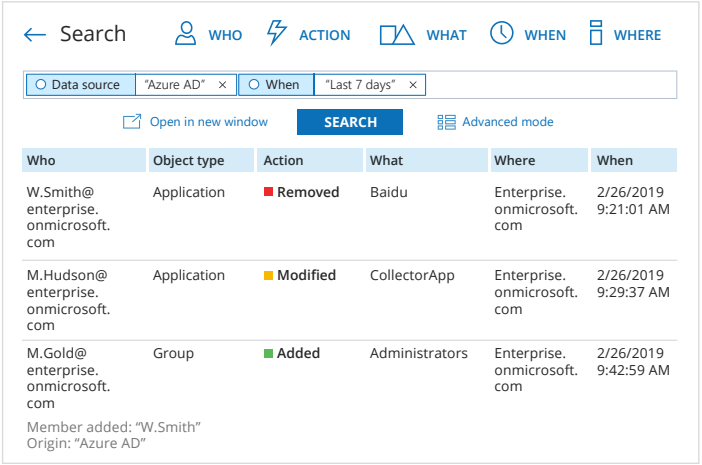
Храните архивные контрольные журналы в сжатом виде более 10 лет в соответствии с требованиями различных нормативов и обеспечьте доступ уполномоченных пользователей к данным журналов в любое время.

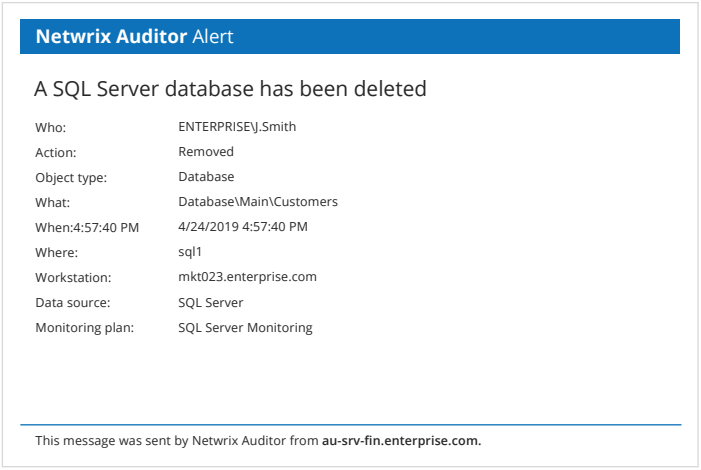
09

Повышайте эффективность работы ИТ-отдела без чрезмерного увеличения нагрузки на сотрудников

Отвечайте на запросы пользователей до возникновения проблем

Если пользователю нужно понять, куда пропал файл и как его вернуть, или почему нет доступа к виртуальной машине, на которой работает критически важное приложение, вы можете найти ответ всего за несколько кликов, чтобы пользователи могли быстро возобновить работу





Быстро реагируйте на события, которые могут привести к простою

Сразу получайте уведомления о таких событиях, как удаление подразделения или базы данных с информацией о клиентах, и устраняйте проблемы, прежде чем они помешают работе компании.

10

Повышайте эффективность работы ИТ-отдела без чрезмерного увеличения нагрузки на сотрудников

Получите четкую картину всех изменений

Контролируйте все изменения в локальных и облачных ИТ-системах, чтобы заранее выявить и устранить проблемы, до того как они станут препятствием для бизнеса и эффективной работы пользователей. Благодаря этому вы сможете гарантировать бесперебойную работу ИТ-сервисов, выполнить SLA и удовлетворить требования пользователей.

Sharing and Security Changes

Shows changes to security group membership, policies, and sharing settings, such as promoting a user to site collection administrator or sharing data with external users.

Action	Object Type	What	Who	When
Modified	Group	GroupName1	T.Simpson @enterprise. onmicrosoft.com	9/1/2018 8:56:10 AM
Where:	https://enterprise-my.sharepoint.com/sites/Test_Do_Not_Delete			
Workstation:	81.09.21.122			
Modified	List	https://enterprise -my.sharepoint.com/ Lists/Customers	T.Simpson @enterprise. onmicrosoft.com	9/1/2018 8:35:44 AM
Where:	https://enterprise-my.sharepoint.com			
Workstation:	81.09.21.122			
Permissions:	• **Added:** "User Account Administrator (Edit)"			

Windows Server Configuration Details

Provides review of Windows server configuration. For a server, the following details are reported: its OS, antivirus, local users and groups, files shares, installed programs, and services. You can apply baseline filters to highlight security issues, such as outdated operating system or improper antivirus. Use this report to examine server configuration details and proactively mitigate risks in your environment.

Category: General

Server	OS Name	OS Version	Antivirus Status
audit.enterprise.com	Microsoft Windows Server 2012 R2 Standard	6.3.9600	Issues Detected

Category: Software

Object Type	Object Name	Properties
Software	Microsoft OneDrive	Available: ENTERPRISE\M.Peterson, Version: 17.3.4604.0120
Software	Trojan	Available: All users, Version: 6.9.5.2956
Software	Google Chrome	Available: All users, Version: 66.0.3359.139
Software	uTorrent	Available: ENTERPRISE\J.Hanson, Version: 3.5.3.44396

Быстро анализируйте настройки систем и выявляйте отступления от базовых требований

Решение позволяет определить текущее состояние критически важных данных быстрее, чем в ручном режиме, чтобы можно было проверить соответствие настроек базовым требованиям и, в случае расхождений, устранить проблемы, чтобы предотвратить вынужденный простой и помехи для пользователей.

11

Повышайте эффективность работы ИТ-отдела без чрезмерного увеличения нагрузки на сотрудников

Отвечайте на вопросы за несколько минут

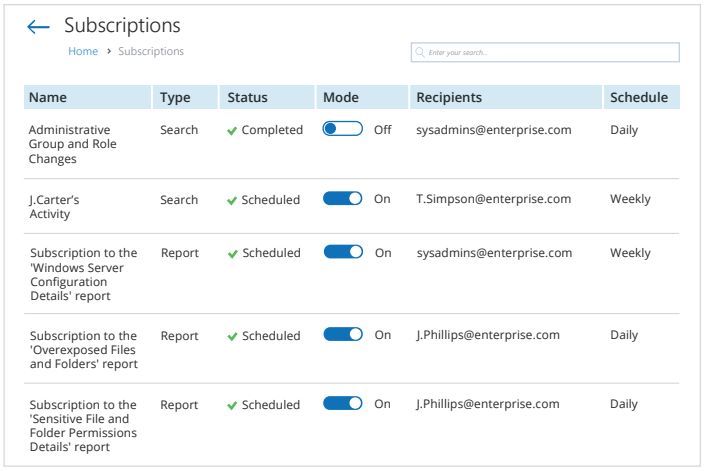
Если руководителям нужна информация, например, перечень тех, кто имел доступ к конкретной папке, или подтверждение того, что в ИТ-среде нет неактивных пользователей, вы можете быстро подготовить удобный для чтения отчет с помощью готового шаблона.

Folder and File Permission Details

Shows permissions granted on a shared folder, its subfolders and files (either directly or via group membership). Use this report to see who has access to a particular folder and its contents, and reveal objects that have permissions different from their parent. Clicking the group link opens the "Group Membership by User" report.

Object: \\fs1\Accounting\Contractors (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\J.Carter	Full Control	Group
ENTERPRISE\T.Simpson	Read (Execute, List folder content)	Group
ENTERPRISE\J.Smith	Full Control	Directly
ENTERPRISE\A.Tompson	Full Control	Group
ENTERPRISE\M.Brown	Full Control	Directly



Избавьтесь от проблем с созданием отчетов

Автоматически отправляйте руководителям информацию в соответствии с удобным для них расписанием. Вы также можете предоставить им доступ к Netwrix Auditor, чтобы они самостоятельно получали необходимую информацию в любое удобное время.

12
Приложения Netwrix Auditor

Проводите аудит главных ИТ-систем централизованно

Больше не нужно переключаться между разными инструментами для создания отчетов и подготовки к аудиту, пытаясь собрать необходимую информацию из всех локальных и облачных систем. Netwrix Auditor предоставляет всю необходимую информацию в стандартизованном виде.

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Exchange
- Netwrix Auditor for Azure AD
- Netwrix Auditor for Office 365
- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for EMC
- Netwrix Auditor for Nutanix Files
- Netwrix Auditor for NetApp
- Netwrix Auditor for SharePoint
- Netwrix Auditor for Windows Server
- Netwrix Auditor for Oracle Database
- Netwrix Auditor for SQL Server
- Netwrix Auditor for Network Devices
- Netwrix Auditor for VMware

13

API интеграции с Netwrix Auditor

Воспользуйтесь широкими возможностями интеграции, аудита и создания отчетов

Централизованный аудит и создание отчетов

Собирайте информацию обо всех действиях в локальных и облачных приложениях и храните все журналы вместе, чтобы отслеживать угрозы для безопасности инфраструктуры, упрощать расследование ИБ-инцидентов и аудитF

Эффективность инвестиций в системы SIEM

Получайте информацию от SIEM в понятном виде и быстрее проводите расследования, вводя в систему данные, собранные Netwrix Auditor и предоставленные в удобной форме.

Автоматизация ИТ-процессов

Интегрируйте Netwrix Auditor с инструментами обеспечения безопасности, соответствия нормативным требованиям и повседневной работы ИТ-отдела, чтобы упростить управление изменениями или инцидентами.

Бесплатные и готовые к использованию дополнения для интеграции Netwrix Auditor с вашей экосистемой вы найдете в Netwrix Add-on Store по ссылке: **netwrix.com/go/add-ons**

14

Почему Netwrix Auditor

Основные причины, по которым заказчики выбирают Netwrix Auditor

Быстрая окупаемость

Решение готово к работе сразу после установки и начинает окупаться с первых же дней. Не платите за дорогостоящие профессиональные услуги и не тратьте время на длительное развертывание.

Адекватная стоимость

Решение продается по разумной цене и позволяет точно спрогнозировать будущие эксплуатационные расходы.

Неинтрузивная архитектура

Вам больше не придется мучиться с агентами и недокументированными способами сбора данных.

Первоклассная техподдержка

Первоклассная служба поддержки быстро и эффективно решает проблемы клиентов — индекс удовлетворенности 97%.

> *«Netwrix Auditor однозначно лучший по соотношению "цена-качество"».*
>
> ИТ-менеджер в финансовой отрасли

Gartner peerinsights

15
Истории Успеха

Узнайте, как заказчики решают свои задачи с помощью Netwrix Auditor

Более 10 000 организаций из разных отраслей по всему миру используют Netwrix Auditor для защиты критически важных для бизнеса данных, прохождения аудита на соответствие стандартам и эффективного управления локальной, облачной и гибридной ИТ-инфраструктурой.

НКО

Netwrix Auditor помог Horizon Leisure Centres обеспечить безопасность конфиденциальных данных и выполнить требования GDPR.

Страхование

First Insurance Company of Hawaii использует Netwrix Auditor для повышения стабильности ИТ-систем и ускорения расследований ИБ-инцидентов.

Еда и Напитки

Компания Perfetti Van Melle Turkey выполнила требования стандарта ISO/IEC 27001 и укрепила внутренние политики безопасности, используя Netwrix Auditor.

Энергетика

Pike Electric ускорила диагностику проблем и обеспечила непрерывную работу с помощью Netwrix Auditor.

О компании Netwrix

Компания Netwrix разрабатывает ПО, которое обеспечивает специалистам в области информационной безопасности и управления полный контроль на конфиденциальными подпадающими под требования нормативов и критически важными для бизнеса данными, , где бы они ни находились. Более 10 000 организаций в разных странах используют решения Netwrix для обеспечения безопасности конфиденциальных данных, максимально эффективного использования корпоративной информации, прохождения аудита на соответствие стандартам с меньшими затратами сил и средств, а также повышения эффективности работы ИТ-отделов и специалистов.

Компания Netwrix была основана в 2006 году. Она удостоена более чем 150 отраслевых наград и включена в списки самых быстрорастущих компаний в США «Inc. 5000» и «Deloitte Technology Fast 500».

Подробную информацию можно найти на сайте www.netwrix.com.

Следующие Шаги

Пробная версия
netwrix.ru/auditor

Персональное демо
netwrix.com/livedemo

Демо в браузере
netwrix.ru/onlinedemo

Главный офис: 300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Netwrix Россия: 197374, Санкт-Петербург, Торфяная дорога д. 7, лит. Ф
Международный: 1-949-407-5125 **Россия:** +7-812-309-54-98

netwrix.com/social