

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

Софтуер за одит на промените в ИКТ средите Netwrix

www.amaccloud.eu

Събирането и съхранението на данни

Тип решение: софтуер
Тип лиценз: вечен (perpetual), с включени 12 месеца поддръжка
Брой лицензи: 350 стандартни лицензи и 250 сервизни лицензи
Работи без да използва агенти , така че да не влияе негативно на производителността на системите и не спира работния процес.
Не се използват никакви недокументирани методи за събиране на данни от системите на организацията, тъй като подобни методи могат да доведат до отказване на поддръжка от Microsoft или от други ключови производители.
Събира сурови машинни данни и ги преобразува в опростена, ясна информация за всяко потребителско действие, за да се улесни вземането на правилни решения от организацията.
Обединява данни от множество източници (логове за събития, извадки от настройките на средите, записи на действията, свързани с промени и т.н.), за да се извлече възможно най-пълната и надеждна одитна информация, без пропуски.
Събира и предоставя пълни детайли за всяка промяна и опит за достъп, включително кога и къде промяната или опита за достъп са направени, кой ги е направил и какво точно е променено или достъпено.
Извършва цялостно сравнение и събира стойностите преди и след промяната за всички променени обекти.
Ползва система за съхранение на данни на две нива (SQL база от данни за отчитане и файлово-базирана система за архивиране на данни в компресиран формат за дълготрайно съхранение). Този архив съдържа цялостна одитна информация за до повече от 10 години, без да намалява производителността на системата, като осигурява лесен достъп до данните за целият период.
Събира одитна информация от локални и от облачни приложения и ги съхранява в защитен, централизиран архив, което позволява използването на общи аларми, търсене, отчитане и анализ на рисковете по сигурността

Поддържани системи и обхват на одитирането

За активната директория (Active Directory) и груповите политики: <ul style="list-style-type: none"> докладва за промени в активната директория и в груповите политики събира информация за промените във времето на активната директория и на груповите политики, включително за участниците в групи с множество домейни и различни права на достъп одитира вписванията поддържа доверени и недоверени домейни
За MS Exchange: <ul style="list-style-type: none"> събира информация за промените на конфигурациите в Exchange Server, Exchange databases, mailboxes, mailbox делегиранията и разрешенията. Одитира достъпа до пощенски кутии без потребител Поддръжка на Exchange 2016
За Windows File Servers:

- докладва за промени по файлове, папки, споделени пространства и права за достъп
- докладва за преместени, преименувани или копирани файлове
- дава информация за успешни и неуспешни опити за прочитане на данни
- дава информация за промените във времето на ефективните права за достъп, включително и кои потребители имат превишени права за достъп
- създава отчети за собствеността на данните, използването на данните и обема на данните, отдавна неизползвани файлове и дублирани файлове
- докладва за чувствителни данни, включително къде са разположени, кой има активни права да ги достъпва и кой е собственик на данните, както и за успешни и неуспешни опити за достъп до данните и опити за промяна на правата за достъп до тях
- поддържа множество файлови сървъри и файлови устройства, разположени в няколко физически обекта, домейна и организации

Одити и аларми

Включва предварително зададени одитни отчети и dashboard-ове, които предоставят детайлна информация за промени, опити за достъп и настройки, представени в четим вид, позволявайки на потребителите да филтрират, сортират и извличат одитните данни.

Позволява на потребителите лесно да изградят **собствен отчет**, базиран на конкретни изисквания, включително отчети, които да обхващат множество, разнообразни системи.

Автоматично изпраща отчети до зададени получатели по email или ги запазва в споделен файлов дял по зададен график (веднъж дневно, седмично, т.н.).

Поддържа извличането на отчети в няколко различни формата, включително PDF, XLS(X), DOC(X) и CSV.

Позволява на потребителите лесно да сортират и филтрират одитната информация чрез Google-подобна интерактивна търсачка, така че те лесно да открият точните данни, които са им необходими.

Показва настоящите настройки на одитираните среди или как са изглеждали настройките в даден отрязък от миналото, включително активните права за достъп на даден потребител или обект, настройките на груповите политики и детайлите за настройките на Windows сървърите.

Включва готови за ползване отчети, които са пригодени за проверяване на съвместимост със стандарти като **ISO/IEC 27001, GDPR, PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST800-53, CJIS, FERPA, NERC CIP** и др.

Известява чрез email или чрез SMS съобщение отговорните екипи за подозрително поведение или събития, които могат да прерастнат в инциденти по сигурността, включително активност, която надвишава изчислените норми (аларми на базата на повторяемост на едно и също събитие).

Може да докладва чрез SQL SRS и може да използва отчетните услуги на SQL сървър по индустриален стандарт (поддържа и безплатната версия SQL Express), за да се предоставя широка гама от одитни отчети.

Сигурността на информацията

<p>Притежава Dashboard-ове за оценяване на ИТ рисковете, които позволяват на потребителите да идентифицират и оценят рисковете по три ключови показателя: управление на акаунти, права за достъп до системите за сигурност и управление на данни.</p>
<p>Притежава Dashboard за откриване на аномално поведение, чрез който се подобрява засичането на зловредни акаунти в ИТ средата, като предоставя агрегирани данни за аномалното потребителско поведение и поставя съответна оценка на риска.</p>
<p>Предоставя отчети за потребителско поведение и за анализиране на пропуските в системите за наблюдение. Предоставя информация за потенциални инциденти, свързани със сигурността, като например действия извън нормалните бизнес часове на деня, необичайни вписвания в системите, голям брой неуспешни опити за действия, достъпване на архивирани данни, действия от досега неактивни потребителски акаунти и наличие на потенциално опасни файлове на файловете сървъри.</p>

Функции от общ характер

<p>Управление на Event logs: Автоматично се събират, обединяват и архивират данните за настъпили събития, така че администраторите могат да одитират събития от общ характер, събития, свързани с услуги, вписвания на потребители и състояли се сесии с отдалечен достъп.</p>
<p>Има Dashboard за здравето на системите и за издаване на ежедневен обобщаващ отчет, който позволява на потребителите да открият проблеми, които влияят на цялостта на събраните одитни данни, като лесно може да се достигне до конкретната детайлна информация, която е необходима, за да се отстранят проблемите. Потребителите могат да получават email отчет веднъж дневно, който да обобщава извършените действия през последните 24 часа.</p>

Интерфейс за управление на системата

<p>Разполага с централизирана конзола за управление, която поддържа множество сървъри, като всеки може да има собствени, различни настройки.</p>
<p>Позволява интегрирането с други решения, поддържа одитирането на множество от системи и приложения, включително системи, които са интегрирани чрез RESTful API, като всичко е обединено, позволявайки използването на dashboard-ове и отчети за комплексни среди от разнообразни системи.</p>
<p>Решението дава цялостен изглед над средата, като всички функционалности са част от единна платформа, премахвайки необходимостта от използването на множество отделни решения.</p>
<p>Правата за достъп са ролево базирани. Платформата позволява фино разделяне на задълженията по наблюдението на системите от различните потребители, така че всеки от тях има достъп само до необходимите му системи и настройки.</p>

Възможностите за интегриране с други решения

<p>Има напълно документиран RESTful API интерфейс за интеграция с други решения и може да се интегрира с решения за сигурност, за съответствие с различни сертификати и за автоматизиране на ИТ процесите и на работата на бизнес приложенията, така че да се предостави централизирано</p>
--

одитиране и отчетност или да се улесни управлението на промените и на действията по поддръжката на системите
Може да се интегрира със SIEM решения , за защита инвестициите на организацията в SIEM платформи, като се предостави интегриране с определени SIEM решения, обогатявайки събраните от тях данни, предоставяйки контекста на събитията
Позволява безплатно да се добавят add-on добавки за интегриране с други решения и има възможност за добавяне на безплатни, предварително създадени add-on добавки, които улесняват интегрирането с решения, като например SIEM, ServiceNow ITSM и Linux системи.

Спецификация на предложените продукти Netwrix

Описание на продукт	SKU	Количество
Netwrix Auditor for Active Directory Support & Maintenance: 12 Months	NW-P-NA-AD	350
Netwrix Auditor for Active Directory - Service Account License Support & Maintenance: 12 Months	NW-P-NA-AD-SA	250
Netwrix Auditor for Windows File Servers Support & Maintenance: 12 Months	NW-P-NA-FS	350
Netwrix Auditor for Windows File Servers - Service Account License Support & Maintenance: 12 Months	NW-P-NA-FS-SA	250
Netwrix Auditor - Active Directory, Exchange & Mailbox Access - Perpetual Support & Maintenance: 12 Months	NW-P-NA-ADEM	350
Netwrix Auditor for Exchange - Perpetual - Service Account License Support & Maintenance: 12 Months	NW-P-NA-EX-SA	250

Процес и стъпки по внедряване на системата Netwrix:

1. Изготвяне на план график за внедряване на системата Netwrix
2. Съгласуване на план графика със специалистите на „АЕЦ Козлодуй“ ЕАД
3. Активиране на продуктите Netwrix, започване на инсталацията, конфигурация и тестването и в ИТ средата на „АЕЦ Козлодуй“ ЕАД в присъствието на служители на „АЕЦ Козлодуй“ ЕАД
4. Контрол на качеството и финални тестове преди пускането в експлоатация на системата Netwrix в ИТ средата на „АЕЦ Козлодуй“ ЕАД
5. Пускане в експлоатация и наблюдение на системата Netwrix в ИТ средата на „АЕЦ Козлодуй“ ЕАД
6. Провеждане на обучение (на място или online) на персонала (до 5 служителя) на „АЕЦ Козлодуй“ ЕАД относно експлоатацията, конфигурирането и инсталирането на системата Netwrix
7. Подписване на приемо-предавателен протокол за извършено успешно внедряване на системата Netwrix в ИТ средата на „АЕЦ Козлодуй“ ЕАД
8. Край на проекта



www.amaccloud.eu

ОФЕРТА

Уважаеми Дами и Господа,

Във връзка с пазарна консултация № 48780 имам удоволствието да Ви предложа нашето специално предложение:

Забележка: Посочените цени на отделните позиции **са без ДДС в ЛЕВА**. ДДС в размер на 20% се начислява отделно за всички стоки и услуги.

Описание на продукт	SKU	Цена за брой	Количество	Общо цена
Netwrix Auditor for Active Directory Support & Maintenance: 12 Months	NW-P-NA-AD	38.86 лв.	350	13,601.00 лв.
Netwrix Auditor for Active Directory - Service Account License Support & Maintenance: 12 Months	NW-P-NA-AD-SA	9.16 лв.	250	2,290.00 лв.
Netwrix Auditor for Windows File Servers Support & Maintenance: 12 Months	NW-P-NA-FS	29.43 лв.	350	10,300.50 лв.
Netwrix Auditor for Windows File Servers - Service Account License Support & Maintenance: 12 Months	NW-P-NA-FS-SA	6.91 лв.	250	1,727.50 лв.
Netwrix Auditor - Active Directory, Exchange & Mailbox Access – Perpetual, Support & Maintenance: 12 Months	NW-P-NA-ADEM	31.23 лв.	350	10,930.50 лв.
Netwrix Auditor for Exchange - Perpetual - Service Account License Support & Maintenance: 12 Months	NW-P-NA-EX-SA	4.31 лв.	250	1,077.50 лв.

39,927.00 лв.



www.amaccloud.eu

Общи условия:

Срок на валидност на офертата: 30 (тридесет) дни от датата на изпращането и;

Срок на доставка: до 20 (двадесет) работни дни;

Начин на доставка: електронно доставени лицензи;

Условия на плащане: до 20 (двадесет) работни дни след доставка на продуктите;

Включени услуги: офертата включва услуги по внедряване, конфигурация, тестване и пускане в експлоатация на избраните решения спрямо план график изготвен съвместно между специалистите на „АЕЦ Козлодуй“ ЕАД и „АМА Клауд Консултинг“ ЕООД;

Обучение: офертата включва обучение на до 5 (пет) специалиста от страна на „АЕЦ Козлодуй“ ЕАД;

Поддръжка: 12 (дванадесет) месеца от срока на активация на продуктите от страна на производителя.

С Уважение,

Марина Попова
Sales Manager

АМА Клауд Консултинг ЕООД
e-mail: project@amaccloud.eu
www.amaccloud.eu



March 28, 2022

Nuclear Power Plant Kozloduy
Bl. 79-B, ar. 42
Kozloduy, Vratsa, 3320
Bulgaria

RE: Manufacturer's Authorization for AMA Cloud Consulting EOOD

To Whom It May Concern,

I am pleased to inform you that Netwrix Corporation ("Netwrix"), the official manufacturer of Netwrix products, hereby confirms that AMA Cloud Consulting EOOD ("AMA") of 47 Narodno Horo str., Sofia, 1618 Bulgaria is a reseller via Netwrix's authorized distributor Computer 2000 Bulgaria Ltd. ("Computer") of 63 Shipchenski prohod Blvd., Fl. 4, Sofia, 1574 Bulgaria.

As a reseller via Computer, AMA can provide Netwrix products to their end users in Bulgaria.

Should you have any questions about this information, please contact Evgenia Izotova, Team Lead - Emerging Markets, at Evgenia.Izotova@netwrix.com or +442035883023 x2252.

Sincerely,

A handwritten signature in black ink, appearing to read "Rachel Richart", is written over a horizontal line.

Rachel Richart
Director of Legal & Corporate Counsel
Netwrix Corporation