Техническа спецификация по обособена позиция № 7

„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“

1. Платформа за защита от изтичане/загуба на данни от крайните точки и от мрежата

Общи изисквания	
REQ.1.	Тип лиценз: абонамент (subscription), с включени 60 месеца поддръжка от производител
REQ.2.	Брой лицензи: 8000
REQ.3.	Решението трябва да разполага с единна централизирана конзола (уеб-базирана конзола, достъпна през уеб браузър, без да изисква инсталирането на допълнителен софтуер), от която да могат да се управляват всички компоненти на DLP: за засичане и спиране на изтичане на данни на мрежово ниво и чрез електронни съобщения (мрежово DLP); за засичане и спиране на изтичане на данни на ниво крайна точка (Endpoint DLP); за откриване и класифициране на данни (Discover).
REQ.4.	Решението да позволява централизирано управление и конфигуриране на политиките за всички продукти (за наблюдение и за превенция, на мрежово ниво и на ниво крайна точка) през уеб-базираната конзола за управление, използвайки еднаква логика за изграждането на политиките им.
REQ.5.	Откъм скалируемост, решението трябва да поддържа надграждане в бъдеще, което да включва управлението на решения за уеб защита и защита на електронна поща, както и на решения за защита на облачни приложения.
REQ.6.	Решението да поддържа интеграция със следните облачни среди: Office365, OneDrive, Box.
REQ.7.	Решението трябва да позволява разполагане на агенти по крайните точки, за засичане и спиране на изтичане на данни на ниво крайна точка, директно от централизираната конзола за управление, използвайки софтуерни методи като GPO, SCCM или други.
REQ.8.	Решението трябва да предоставя информация в централизираната конзола за състоянието на имплементираните агенти по крайните точки, като да информира ако даден агент не функционира правилно.
REQ.9.	Решението да поддържа имплементация на компонентите в Hyper-V или VMware среда.
REQ.10.	Да могат да се създават потребителски акаунти за достъп до решението, като да могат да им се задават различни права за достъп (например даден потребител само да може да преглежда инциденти от конкретни системи, но не и да извършва действия с тях). Да се поддържа ролево-базирана администрация.
REQ.11.	Решението да може да се интегрира с активна директория и да поддържа двуфакторна автентикация.
REQ.12.	Всички компоненти на решението да могат да се конфигурират и обновяват директно от централизираната конзола за управление.

REQ.13.	Решението да може да се интегрира със скачено хранилище за данни (SAN), което да позволява дълготрайно съхранение на събраните сурови данни и метаданни, за покриване на изисквания от различни регулации.
REQ.14.	Решението трябва да предоставя общ графичен изглед в централизираната конзола за управление, които да показва всички инциденти с данни, разделени по степен на риск, тип събития и т.н. Инцидентите да могат да се разследват директно от конзолата за управление.
REQ.15.	Решението да позволява ескалирането на инциденти от критична важност за организацията към определени екипи или отговорни лица, директно от централизираната конзола за управление.
REQ.16.	Всички дейности, свързани с работата на администраторите с възникналите инциденти, да се отчитат и да са видими в централизираната конзола за управление.
REQ.17.	Решението трябва да позволява извличането на файловете с логираните данни за работата му в различни формати, за допълнителен одит. Файловете с логирани данни да са защитени от неправомерно подменяне на информация.
REQ.18.	Решението трябва да може да търси класифицирани данни (Discover) по зададени критерии, като трябва да се запомнят откритите досега данни и при последващо сканиране да се търсят само нови данни, които не са индексирани.
REQ.19.	Решението да може да поставя пръстови отпечатъци (fingerprint) на засечени файлове с класифицирани данни. Хеш сумите на отпечатъците да се съхраняват в база от данни и да могат да се използват за търсене и за изграждане на политики за сигурност.
REQ.20.	Решението да може да използва единна политика за сканиране на данни, независимо от това къде се намират (data-at-rest), къде се трансферират (data-in-motion) или как се използват (data-in-use), както на мрежово ниво, така и на ниво крайна точка. Системата автоматично да може да предприема съответни действия, според засечената заплаха от изтичане на данни.
REQ.21.	Решението да позволява поставянето на оценка на риска от даден инцидент, според количеството класифицирани данни, с които се работи неправомерно, базирайки се на политиките на организацията.
REQ.22.	Решението да разполага с предварително зададени политики, за засичане на неправомерни действия с класифицирани данни, които да отговарят на изискванията на различни регламенти за обработка на данни. Предварително зададените политики да са по категории, според регион и тип индустрия.
REQ.23.	Решението да разполага с предварително зададени политики, които да индикират за неправомерни действия с данни от потребителите на организацията, водещи до риск от изтичане на данните.
REQ.24.	Да се предоставят поне 1500 предварително зададени политики, за да не е необходимо отделянето на много време от администраторите в създаване на собствени политики.
REQ.25.	Решението трябва да позволява задаването на изключения в политиките, за да може да се изключат дадени обекти от сканиране и блокиране и за да се сведат грешните показания до минимум. Да може да се избира на кои приложения им се има доверие да достъпват данни.
REQ.26.	Решението трябва да позволява задаване в политиките за сигурност на държави, към които винаги да е забранен износа на данни по мрежата, освен ако не са конфигурирани изключения.

REQ.27.	Създаването и управлението на политиките трябва да става лесно, през графичния интерфейс за централизирано управление на решението, без да е необходимо използването на сложни скриптове.
REQ.28.	Решението трябва да позволява лесно да се изграждат правилата в политиките за сигурност, като да могат да се използват ключови думи или регулярни изрази (regular expressions), използвайки стандартна булева логика.
REQ.29.	Решението да може да извлича и инспектира текстовото съдържание от файлове и от прикачени файлове в електронни съобщения. Да се предостави пълен списък на поддържаните файлови типове.
REQ.30.	Решението да може да обработва съдържание на кирилица.
REQ.31.	Решението да може да сканира съдържанието на архиви (ZIP, TAR, RAR файлови формати), на до 16 нива навътре при вложени архиви, като да може да засича наличието на класирана информация в тях.
REQ.32.	Решението да може да обработва много големи файлове (от 20MB нагоре) при сканирането за класифицирани данни.
REQ.33.	Решението да може да засича множество случаи на изтичане на данни във времето, породени от един и същ потребител, като да може да създаде общ инцидент при достигане на определено, зададено количество събития. По този начин решението трябва да може да засича опити за частично изнасяне на информация от дадени потребители за дълъг период от време.
REQ.34.	Решението да може да засича изтичане на данни от структурирани системи, което включва бази данни от типа Microsoft SQL Server, Oracle, IBM DB2, както и да всички други типове бази данни, можещи да използват ODBC или OLE конектори за свързване с трети системи.
REQ.35.	Решението да може да прави разлика между различни типове PII или PHI числа при засичането на класифицирани данни. Например, решението да може да прави разлика между деветцифрен номер за социално осигуряване от деветцифрен телефонен номер, без да е необходимо пред числото да има ключова дума, под формата на текст, който да го обособява (например текста „тел. номер“).
REQ.36.	Решението да разполага с machine-learning технология (да използва алгоритми и техники, за да може автоматично да се учи от предишни инциденти)
REQ.37.	Решението да може да използва бели списъци със зададено текстово съдържание, което да се игнорира при сканирането за заплахи.
REQ.38.	Решението да може да сканира за мрежови заплахи за данните в Microsoft Exchange 2013 среда и да може да ги предотвратява.
REQ.39.	Решението да може да работи с класифицирани данни, съдържани във файловете, съхранени в SharePoint 2013 среди.
REQ.40.	Решението да може да открива класифицирани данни по мрежата за Exchange Online и SharePoint Online (Office 365) среди. Решението да може да се интегрира чрез API интерфейса на Microsoft за Office 365.
REQ.41.	Решението да може да работи с описано съдържание под формата на ключови думи и фрази, както и изрази от типа regular expressions.

REQ.42.	Решението да може да засича и блокира криптиран пренос на данни. Да се опишат какви типове криптирана комуникация се поддържат.
REQ.43.	Решението да може да извлича и обработва съдържанието от графични файлови формати, използвайки OCR технология, като например Abbyy FineReader или Nuance. OCR технологията трябва да е вградена в решението, без да е необходимо закупуването на допълнителни лицензи.
REQ.44.	Решението трябва да може да съхранява информация за засечените данни заедно с прилежащите им метаданни (време и дата на инцидента, потребител предизвикал инцидента, използвани протоколи за пренос на данни и т.н.)
REQ.45.	Решението да може да изпраща автоматични аларми под формата на електронни съобщения.
REQ.46.	Решението да може автоматично да завишава степента на риск на даден инцидент (и съответните аларми) ако той се повтори зададен брой пъти в зададен период от време.
REQ.47.	Решението да може автоматично да известява потребителите или техните ръководители, когато нарушат дадена политика.
REQ.48.	Решението да може да предоставя известие на екрана на работната станция на даден потребител, когато той наруши политика, отнасящата се за работата с класифицирани данни за крайни точки.
REQ.49.	Да могат да се задават автоматични действия от системата по различни параметри, например коя политика е нарушена, степента на риска на инцидента, броя събития, използвания протокол за комуникация и т.н.
REQ.50.	Решението да може автоматично да може да копира файловете в карантина, да криптира файловете (допуска се използването и на third-party инструменти за криптиране) или да трие файловете, които са засечени при неправомерни действия.
REQ.51.	Инцидентите директно да могат да се разследват от централизираната конзола за управление.
REQ.52.	Инцидентите ясно да могат да показват причината и конкретните данни, които са довели до нарушаване на политиката, а не само коя политика е нарушена.
REQ.53.	Решението да дава възможност да се освободят (маркират като грешни показания) група инциденти наведнъж от засечените заплахи, например да се освободят множество електронни съобщения от карантината наведнъж.
REQ.54.	Решението да може да дава информация и да изготвя отчети, които да информират кои инциденти и кои потребители носят най-голям риск за организацията и кои инциденти трябва да се разгледат първи, с по-голям приоритет.
REQ.55.	Отчетите да могат да се извличат от системата в различни файлови формати, например PDF и CSV.
REQ.56.	Дадени потребители или група от потребители да могат да се абонират за автоматично получаване на дадени отчети от системата, които да се изпращат по email. Да може да се зададе график (дневно, седмично, месечно и т.н.)
REQ.57.	Всички отчети да са видими и да могат да се управляват от централизираната конзола за управление.

REQ.58.	Решението да разполага с множество отчети по подразбиране (out-of-box), които да покриват най-често срещаните потребности.
REQ.59.	Решението трябва да позволява на администраторите създаването на собствени отчети.
REQ.60.	Решението да може да сканира и блокира (или друго зададено автоматично действие) изходящ уеб трафик, който нарушава политиките за сигурност.
REQ.61.	Решението да може да сканира уеб-трафик за заплахи, включително уеб-базирана поща, уеб-публикации, други протоколи, които използват HTTP и HTTPS, включително прикачени файлове.
REQ.62.	Решението да може да наблюдава и предотвратява опити за уеб-принтиране на класифицирана информация.
REQ.63.	Решението да предоставя детайлна информация за уеб-страниците (не само IP адрес), към които е направен опит за изнасяне на класифицирана информация, включително информация за географското им разположение, като параметрите да могат да бъдат използвани за финна настройка на политиките за сигурност.
REQ.64.	Решението по подразбиране да може да инспектира криптирана SSL комуникация, без тази функция да изисква закупуването на допълнителни модули или да е зависима от използването на ICAP протокол.
REQ.65.	Решението да може да наблюдава уеб-трафика, породен от приложения за комуникация на потребителите (instant messaging), дори когато този трафик преминава по порт 80.
REQ.66.	Решението трябва да може да сканира и блокира (или друго зададено автоматично действие): чувтствителни данни в SMTP трафик, прикачена чувствителна информация към уеб трафик, пренос на чуствителни данни от файлов сървър към работна станция (LAN трафик), пренос на чувствителна информация в PDF формат.
REQ.67.	Решението да може да сканира и блокира (или друго зададено автоматично действие) изходящи електронни email съобщения, които нарушават политиките за сигурност.
REQ.68.	Решението да може да наблюдава и налага политики на email трафика, явяващ се вътрешен за организацията (между служители), включително да се сканират прикачените файлове в съобщенията. Да има интеграция с Microsoft Outlook и IBM Lotus Notes.
REQ.69.	Решението да може да поставя в карантина електронните съобщения, които нарушават политиките за сигурност на класифицираните данни на организацията. Да има възможност за ръчно освобождаване на електронни съобщения от карантината.
REQ.70.	Решението да може да анализира трафика, преминаващ през Mail Transfer Agent (MTA)
REQ.71.	Решението да може да засича и блокира (или друго зададено автоматично действие) опити на потребители за копиране на класифицирани данни на преносими устройства (например USB устройства, флопи дискове, CD/DVD, т.н.). Да може да се блокира преноса на данни, независимо дали потребителската крайна точка се намира в или извън мрежата на организацията.
REQ.72.	Решението да може да засича и блокира (или друго зададено автоматично действие) опити на потребители или на приложения да извличат класифицирани данни чрез clipboard, print screen команди и други сходни методи.
REQ.73.	Агента за защита на крайните точки да поддържа работа с крайни точки като Windows Server 2016 и Windows 10 (1709, 1803, 1809, 1903), както и с MacOS.

REQ.74.	Решението да може да се интегрира напълно с трети решения като Titus, Boldon James или Microsoft Azure Information Protection, с цел поставяне на етикети на класифицираните данни.
REQ.75.	Решението за защита от изтичане на данни от крайните точки да може да обработвка класифицирана информация, дори когато крайната точка се намира извън мрежата на организацията.
REQ.76.	Решението да позволява налагането на политики за сигурност на структурирани и на неструктурирани данни, дори когато крайната точка се намира извън мрежата на организацията.
REQ.77.	Решението за защита от изтичане на данни от крайните точки да позволява създаването на bypass пароли, които да позволяват локално или отдалечено временно да се спира работата на агента за сигурност на решението (да не се анализират или блократ действия временно на дадената крайна точка).
REQ.78.	Решението за защита от изтичане на данни от крайните точки да позволява извеждането на диалогов прозорец на крайните точки при дадени действия, който да очаква отговор от потребителите с обосноваване на причините за действието с класифицирани данни.
Гаранция и поддръжка:	
REQ.79.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.80.	Получаване на нови версии на софтуера - 5 (пет) години.