**ՏԵԽՆԻԿԱԿԱՆ ԲՆՈՒԹԱԳԻՐ**

***Հակավիրուսային համակարգչային ծրագրային փաթեթներ «Վերջնական կետերի և սերվերների հակավիրուսային պաշտպանության» ծրագրի 500 հանգույցների համար:***

**Ընդհանուր պահանջներ**

«Վերջնական կետերի և սերվերների հակավիրուսային պաշտպանության» ծրագրի 500 հանգույցների համար:

* Ներկայացված արտադրողը պետք է լինի Gartner magic quadrant լիդերների ցանկում:
* Մատակարարը պետք է իրականացնի տեղադրման և կարգաբերման աշխատանքները:
* Մատակարարը պետք է ներկայացնի արտադրողի կողմից ավտորիզացման նամակ MAF կամ DAF:

**Վերջնական կետերի և սերվերների պաշտպանության հակավիրուսային համակարգի տեխնիկական պահանջներ**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Չափորոշիչ | | Ֆունկցիոնալ նկարագրություն |
| 1. Թարմացում, կառավարում և հաշվետվություն | | | |
|  | Համակարգի կենտրոնացված կառավարում | | * Կենտրոնացված կառավարում մեկ կոնսոլից աշխարհագրորեն ցրված կայքերի համար` կլայենտների(customer) տարբեր խմբեր ստեղծելու և կլայենտների(customer) խմբերին իրենց սեփական քաղաքականությունը վերագրելու հնարավորությամբ: * Բազմաթիվ ադմինիստրատորների կառավարման վահանակի մուտքի տրամադրում և յուրաքանչյուր ադմինիստրատորի համար մուտքի մակարդակի և կլայենտների(customer) խմբերի սահմանում, որոնց նա կարող է կառավարել: * Զանգվածային վարակների հայտնաբերում և ադմինիստրատորների ծանուցում: * Ինտեգրում Active Directory- ի հետ: * Ստեղծել լրացուցիչ տարածք կլայենտի(customer) խմբի համար ՝ հիմնվելով տարբեր պարամետրերի վրա, ներառյալ օգտագործված ցանցային կապի տեսակը, անլար կապի ID- ն, տիրույթի անունների թույլատրումը IP- ին և այլն, և նշանակել սեփական քաղաքականություն լրացուցիչ տեղակայման համար: |
|  | Կլայենտի կողմից թարմացման կառավարում | | * Կառավարման սերվերում թարմացումները ներբեռնելու և դրանք կլայենտներին(customer) բաժանելու ժամանակն ու ժամանակահատվածը սահմանելու հնարավորություն: * Հեռավար կայքերում կլայենտների(customer) համար բովանդակության բաշխման կետ (թարմացման գործիքներ) նշանակելու հնարավորություն՝ թարմացումների բաշխումն օպտիմալացնելու համար: * Շարժական կլայենտների(customer) համար (նոութբուքեր), որոնք կորպորատիվ ցանցից դուրս են, ուղղակիորեն թույլատրել վաճառողի կայքի բովանդակության թարմացումները: |
|  | Կլայենտի կողմից պաշտպանություն | | * Կլայենտին(customer) ջնջելու կամ բեռնաթափելու համար գաղտնաբառի քաղաքականություն սահմանելը: * Կլայենտի(customer) պաշտպանություն չարտոնված ընդհատումից: * Կլայենտի(customer) կազմաձևի ամբողջականության պաշտպանություն: |
|  | Կլայենտի կողմի տեղադրում և կառավարում | | Տեղադրում:   * Կլայենտի(customer) տեղադրումից կամ տեղահանելուց հետո համակարգիչը վերագործարկելու անհրաժեշտության բացակայություն: * Կլայենտի(customer) «լուռ» տեղադրման հնարավորություն: * Կլայենտի(customer) բաշխման հավաքածուի ստեղծում` նշված պարամետրերով (կլայենտին տեղափոխել նշված խումբ, սկանավորել տեղադրման ընթացքում և այլն): * Ապրանքի նոր տարբերակին անցնելը և փաթչ տեղադրումը պետք է տեղի ունենա օգտագործողների համար անտեսանելի ռեժիմով, այսինքն՝ առանց ծանուցումների և վերբեռնումների: * Առանց հակավիրուսների համակարգիչների հայտնաբերում:   Վերահսկում:   * Կախված համակարգչի ծանրաբեռնվածությունից՝ սկանավորման գրաֆիկի, գործարկման պայմանների կարգավորումների հնարավորություն: * Բացառություններ (ֆայլեր, գրացուցակներ, ծրագրեր) ավելացնելու հնարավորություն: |
|  | ՀՎՊ մոդուլի ֆունկցիոնալությունը կարգավորելու ունակություն | | Հնացած կամ թույլ համակարգիչների համար «թեթև» կլայենտի(customer) տարբերակի առկայություն և լրացուցիչ ֆունկցիոնալ մոդուլներ անջատելու հնարավորություն`ՀՎՊ մոդուլի շահագործումն օպտիմալացնելու համար: |
|  | Սպառված ռեսուրսների օպտիմալացման հնարավորություն | | Նվազեցնել պրոցեսորի և մուտքի / ելքի ընդհանուր սպառման ծավալը ` բացառելով սկանավորման «տեղեկատու» ֆայլերի և սկանավորված ֆայլերի ընդհանուր քեշի օգտագործումը |
| 1. **Սարքերի օգտագործման վերահսկում** | | | |
|  | Սարքերի օգտագործման սահմանափակման ֆունկցիոնալությունը | | Սարքերի օգտագործման սահմանափակում՝ ըստ սարքի դասի կամ նույնացուցիչի |
|  | USB-ի հասանելիության սահմանափակման մակարդակները | | Մուտքը արգելափակված է, մուտք միայն կարդալու, կարդալու և խմբագրելու, USB կրիչից հավելվածներ գործարկելու համար |
|  | Ըստ ցուցակների USB սարքերով կենտրոնացված կառավարելու հնարավորություն | | «USB սարքերի սպիտակ ցուցակի» կենտրոնացված սպասարկում |
| 1. Պաշտպանություն վիրուսներից և այլ պառնալիքներից | | | |
|  | | Պաշտպանություն վիրուսներից | Վնասակար ծրագրային ապահովման հայտնաբերման և հեռացման բարձր ցուցանիշ:  Պաշտպանական տեխնոլոգիաների օգտագործումը   * Համաշխարհային ինտելեկտուալ ցանցի տվյալների հիման վրա հեղինակության վերլուծություն * Պարբերաբար թարմացվող բովանդակության հիման վրա ստորագրությունների վերլուծություն * Մեքենայացված ուսուցման տվյալների հիման վրա վերլուծություն * Էմուլատոր, որը հայտնաբերում է վնասակար ծրագրային ապահովում, որի կոդը թաքցնում են փաթեթավորողները * Կեղծ դրական արդյունքների նվազագույնի հասցնելու ծրագրերի վարքային վերլուծություն` չարամիտ և օրինական գործողությունների գնահատման ճանապարհով * Հիշողության շահագործման պաշտպանություն |
| 1. **Մատենագրում** | | | |
|  | Իրադարձությունների գրանցումն ըստ տեսակների | | Իրադարձությունների տեսակները։   * Վնասակար ծրագրերի հայտնաբերման փաստեր (հաջող կամ անհաջող բուժման նշանով, վիրուսի անվանումը և դրա տեղադրման ամբողջական ուղին, ՀՎՊ տվյալների բազաների տարբերակը) * Համակարգի թարմացման փաստեր (նշելով հաջողությունը / ձախողումը, պատճառները, ՀՎՊ տվյալների բազաների ընթացիկ տարբերակը և միջուկի տարբերակը) * ՀՎՊ համակարգի և ամբողջ համակարգի առանձին մոդուլների միացման / անջատման փաստեր (նշելով, թե որ մոդուլներն են միացված / անջատված) |
|  | Մատենագրման պարամետրեր | | Նվազագույն տեղեկատվություն իրադարձություններում:   * Իրադարձության ամսաթիվը / ժամանակը * Անվանում * Իրադարձության նկարագրում * Համակարգչի IP հասցեն, որի վրա տեղի է ունեցել իրադարձությունը * Համակարգչի անվանումը * Համակարգչի մոտ աշխատող օգտատիրոջ անունը * Լրացուցիչ տեղեկություն |
|  | Իրադարձությունների գրանցումն ըստ տեսակների | | Իրադարձության տեսակները:   * Համակարգի լրացուցիչ մոդուլների կանոնների մշակման փաստեր (Firewall, IPS։ կանոնի անվանումը, հասցեն և աղբյուրի նպատակակետ/անվնումը) * USB կրիչներ օգտագործելու փորձերի փաստեր (հաջող / անհաջող, ո՞ր կրիչը և ի՞նչ տվյալներ են գրվել / կարդացել) |
| 1. **Պաշտպանության լրացուցիչ մոդուլներ** | | | |
|  | Firewall(հրապատ)ի մոդուլ | | Կենտրոնականորեն վերահսկվող SPI- հրապատ, որը թույլ է տալիս սահմանել կարգավորումներ համակարգիչների տարբեր խմբերի համար` գործառնական ռեժիմների ընտրության հնարավորությամբ․   * արգելափակել այն ամենը, ինչը չի թույլատրվում * արգելափակել արգելվածը * մատյանում այն փաթեթների գրանցում, որոնք ենթարկվում են կանոններին |
|  | IPS մոդուլ | | * Կենտրոնացված կառավարվող IPS մոդուլ՝ որը հիմնված է թարմացվող ստորագրությունների վրա և օժտված է կանոնները միացնելու / անջատելու հնարավորությամբ: * Սեփական IPS ստորագրության ստեղծում՝ օգտագործելով SNORT- ի նման լեզու: * IPS- ն պետք է վերահսկի մուտքային և ելքային կապերը: |
|  | Հավելվածների  վերահսկում | | * Հավելվածների վերահսկման կենտրոնականորեն կառավարվող մոդուլը, որը թույլ է տալիս վերահսկել գործընթացները ֆայլերի, ռեգիստրի հասանելիության մակարդակում, այլ գործընթացների գործարկումը և դադարեցումը և DLP բեռնումը: * Հավելվածների վերահսկման պատրաստի կանոնների առկայություն՝ հայտնի վնասակար կամ պոտենցիալ վտանգավոր վարքագիծը արգելափակելու համար: * Հավելվածների վերահսկման սեփական կանոնները ստեղծելու հնարավորություն: |
|  | Ամբողջականության վերահսկում | | * Կենտրոնականորեն կառավարվող ամբողջականության վերահսկման մոդուլը * Հակավիրուսային ամբողջականության վերահսկում * Պատրաստի կաղապարների հիման վրա OՀ- ի և հավելվածների կազմաձևման պարամետրերի վերահսկում * ՕՀ-ի և հավելվածների կամայական կազմաձևման պարամետրերի ամբողջականության վերահսկում: * Հավելվածների «սեւ» և «սպիտակ» ցուցակների ստեղծում: * Ինտեգրում ցանցի անվտանգության դարպասների հետ `բաց REST API- ի միջոցով հավելվածների սեւ ցուցակը թարմացնելու համար: * Հավելվածների համար բացառություններ ստեղծելու հնարավորություն, որոնք կկատարվեն ցնկացած դեպքում, այդ թվում `թվային ստորագրության հիման վրա: |
|  | ԾԱ վնասակար ծուղակներ | | * Վնասակար ծրագրերի համար պատրաստի թակարդներ օգտագործելու հնարավորություն: * Վնասակար ծրագրերի համար սեփական թակարդներ ստողծելու հնարավորություն: |
| 1. **Լրացուցիչ ընտրանքներ** | | | |
|  | Ծրագրերի մեկուսացում | | Հակավիրուսային գործիքի միջոցով Windows- ի աշխատանքային կայաններում հավելվածների մեկուսացման տեխնոլոգիա կիրառելու հնարավորություն: |
|  | ՕՀ-ի կարծրացում | | Հակավիրուսային գործիքի օգտագործմամբ Windows- ի կայաններում ՕՀ-ի կարծրացման տեխնոլոգիա կիրառելու հնարավորություն: |
|  | EDR | | Հակավիրուսային գործիքի միջոցով Windows- ի կայաններում և սերվերներում (Վերջնակետի հայտնաբերում և արձագանքում) EDR տեխնոլոգիա կիրառելու հնարավորություն: |

## 

## Общие требования

«Антивирусная защита конечных точек и серверов» программное обеспечение на 500 узлов․

* Поставщик должен предоставить авторизационное письмо от производителя MAF или DAF
* Представленный производитель должен быть в списке Gartner magic quadrant.
* Поставщик должен выполнить работы по установке и настройке продукта․

## Технические требования к антивирусной защите конечных точек

|  |  |  |  |
| --- | --- | --- | --- |
| № | Параметр | | Функционал |
| 1. **Обновление, управление и отчетность** | | | |
|  | Наличие централизованного управления системой | | * Централизованное управление из единой консоли для территориально разнесенных площадок с возможностью создания различных групп клиентов и назначения группам клиентов собственных политик. * Предоставление доступа к консоли управления нескольким администраторам и определение для каждого администратора уровня доступа и групп клиентов, которыми он может управлять. * Определение массовых заражений и уведомления администраторов. * Интеграция с Active Directory. * Создание дополнительных расположений для группы клиентов на основании различных параметров, включая тип используемого сетевого соединения, идентификатор беспроводной сети, разрешение доменного имени в IP и т.д., и назначение собственных политик для дополнительных расположений. |
|  | Управление обновлениями клиентской части | | * Возможность устанавливать время и период загрузки обновлений на управляющий сервер и распространения их на клиенты. * Возможность для клиентов на удаленных площадках назначать точку дистрибуции контента (агенты обновлений) для оптимизации распространения обновлений. * Для мобильных клиентов (ноутбуки), при условии нахождения их за пределами корпоративной сети, разрешать обновления контента с сайта вендора напрямую. |
|  | Защита клиентской части | | * Установка по политике пароля на удаление или выгрузку клиента. * Защита клиента от несанкционированной остановки. * Защита целостности конфигурации клиента. |
|  | Установка и управление клиентской части | | Установка:   * Отсутствие необходимости перезагружать ПК после установки или удаления клиента. * Возможность «тихой» установки клиента. * Создание дистрибутива клиента с заданными параметрами (перемещать клиента в заданную группу, запуск сканирования при установке и т.д.). * Переходы на более новую версию продукта и установка патчей должны проходить в незаметном для пользователей режиме, т.е. без уведомлений и перезагрузки. * Определение компьютеров без антивируса.   Управление:   * Возможность настройки графика сканирования, условий запуска в зависимости от загруженности компьютера. * Возможность добавлять исключения (файлы, директории, программы). |
|  | Возможность настройки функционала модуля АВЗ | | Для устаревших или слабо мощных компьютеров наличие «облегченной» клиентской версии и возможность отключения модулей дополнительного функционала для оптимизации работы модуля АВЗ |
|  | Возможность оптимизации потребляемых ресурсов | | Уменьшение общего объема потребления ресурсов процессора и ввода-вывода путем исключения «эталонных» файлов из сканирования и использования общего кэша просканированных файлов |
| 1. **Контроль использования устройств** | | | |
|  | Функционал ограничения использования устройств | | Ограничение использования устройств по классу устройств или их идентификаторам |
|  | Уровни ограничения доступа к USB | | Доступ заблокирован, доступ только на чтение, доступ на чтение и редактирование, доступ на запуск приложений с USB-накопителя |
|  | Возможность централизованного управления USB-устройствами по спискам | | Централизованное ведение «белого списка USB устройств» |
| 1. **Защита от вирусов и других угроз** | | | |
|  | | Защита от вирусов | Высокий показатель обнаружения вредоносного программного обеспечения и его удаления.  Использование технологий защиты:   * Анализ репутации на основе данных глобальной интеллектуальной сети; * Анализ по сигнатурам на основе регулярно обновляемого контента; * Анализ на основе данных машинного обучения; * Эмулятор, детектирующий вредоносное ПО, код которого скрыт при помощи упаковщиков; * Поведенческий анализ приложений с минимизацией ложных срабатываний путем оценки злонамеренных и легитимных действий; * Защита от эксплойтов памяти; |
| 1. **Журналирование** | | | |
|  | Регистрация событий по типам | | Типы событий:   * Факты обнаружения вредоносного ПО (с отметкой успешного или неуспешного лечения, названия вируса и полного пути его размещения, версии баз АВЗ) * Факты обновления системы (с уточнением успех/не успех, причины, текущая версия баз АВЗ и версия ядра) * Факты включения/отключения отдельных модулей системы АВЗ и всей системы в целом (с указанием какие модули были включены/отключены) |
|  | Параметры журналирования | | Минимальная информация в событиях:   * Дата/время события * Название * Описание события * IP-адрес компьютера на котором произошло событие * Имя компьютера * Имя пользователя, работающего на компьютере * Дополнительная информация |
|  | Регистрация событий по типам | | Типы событий:   * Факты отработки правил дополнительных модулей системы (Firewall, IPS: название правила, адрес и порт источника/назначения) * Факты попыток использования USB-накопителей (успешно/не успешно, какой накопитель и какие данные были записаны/прочитаны) |
| 1. **Дополнительные модули защиты** | | | |
|  | Модуль Firewall | | Централизованно управляемый SPI-firewall, позволяющий задавать настройки для разных групп компьютеров, с возможностью выбора режимов работы:   * блокирование всего, что не разрешено * блокирование того, что запрещено * фиксация в журнал тех пакетов, которые попадают под правило |
|  | Модуль IPS | | * Централизованно управляемый модуль IPS на основе обновляемых сигнатур с возможностью включения/отключения правил. * Создания собственных сигнатур IPS с использованием языка на подобии SNORT. * IPS должен контролировать входящие и исходящие подключения. |
|  | Контроль приложений | | * Централизованно управляемый модуль контроля приложений, позволяющий контролировать процессы на уровне доступа к файлам, реестру, запуска и остановки других процессов и загрузки DLP. * Наличие готовых правил контроля приложений, позволяющих блокировать известные вредоносные или потенциально опасные поведения. * Возможность создания собственных правил контроля приложений. |
|  | Контроль целостности | | * Централизованно управляемый модуль контроля целостности. * Контроль целостность антивируса. * Контроль параметров конфигурации ОС и приложений на основе готовых шаблонов. * Контроль целостности произвольных параметров конфигурации ОС и приложений. * Создание «черного» и «белого» списка приложений. * Наличие интеграции с сетевыми шлюзами безопасности для обновления черного списка приложений через открытый REST API. * Возможность создания исключений для приложений, которые будут выполняться в любом случае, в том числе на основании цифровой подписи. |
|  | Ловушки вредоносного ПО | | * Возможность использовать готовые ловушки для вредоносного ПО. * Возможность создавать собственные ловушки вредоносного ПО. |
| 1. **Дополнительные опции** | | | |
|  | Изоляция приложений | | Наличие возможности на рабочих станциях Windows применить технологию изоляции приложений, используя антивирусный агент. |
|  | Харденинг ОС | | Наличие возможности на рабочих станциях Windows применить технологию харденинга ОС, используя антивирусный агент. |
|  | EDR | | Наличие возможности на рабочих станциях и серверах Windows применить технологию EDR (Endpoint Detection and Response), используя антивирусный агент. |