***Հավելված 1․***

* RAR, ARJ, ZIP, CAB, LHA, JAR, ICE ֆորմատով արխիվային ֆայլերի հակավիրուսային ստուգում և բուժում, այդ թվում գաղտնաբառով պաշտպանված:
* Սկավառակի ամբողջական կոդավորում հատուկ բեռնման մոդուլի ստեղծման և Single Sign On տեխնոլոգիայի աջակցությամբ: Օպերացիոն համակարգի ֆայլերի կամ բեռնման մոդուլի վնասման դեպքում կոդավորված պարունակության վերականգնման հնարավորությամբ գործիքներ: Պետք է գործի UEFI համակարգի հնարավորություն:
* Սկավառակի ամբողջական կոդավորման դեպքում երկֆակտոր վավերացման հնարավորություն
* Ֆայլերի կոդավորում` կոդավորվող բովանդակության ճկուն նշման ունակությամբ (տեղադրման տեղակայման միջոցով, ընդլայնման միջոցով, ֆայլ ստեղծող հավելվածի միջոցով): Ընտրվածհավելվածների կողմից կոդավորված ֆայլերի հասանելիությունը սահմանափակելու մեխանիզմներ, ինչպես նաև տեխնոլոգիաների առկայություն, որը թույլ է տալիս ապակոդավորել ֆայլերըչպաշտպանված միջավայրում գաղտնաբառի միջոցով:
* Տվյալների կոդավորում շարժական կրիչների վրա, գործառնական ռեժիմը սահմանելու ունակությամբ, որը թույլ է տալիս կոդավորել և վերծանել ֆայլերը կազմակերպության ցանցից դուրս:
* Պաշտպանություն ծրագրային ծառայության չարտոնված հեռահար կառավարումից, ինչպես նաև ծրագրի պարամետրերի մատչման պաշտպանություն գաղտնաբառի միջոցով՝ վնասակար ծրագրերից, ներխուժումներից և արտոնություն չունեցող օգտվողներից
* Հակավիրուսային պաշտպանության միայն ընտրված մոդուլների տեղադրման հնարավորություն

**Ընդհանուր պահանջներ**

Հակավիրուսային միջոցները պետք է ներառեն.

• Հակավիրուսային ծրագրային պաշտպանություն Windows կայանների համար

• Հակավիրուսային ծրագրային պաշտպանություն MacOS կայանների համար

• Հակավիրուսային ծրագրային պաշտպանություն Linux կայանների համար

• Հակավիրուսային ծրագրային պաշտպանություն Windows ֆայլային սերվերների համար

• Հակավիրուսային ծրագրային պաշտպանություն Linux ֆայլային սերվերների համար

• Հակավիրուսային ծրագրային պաշտպանություն շարժական սարքերի համար (սմարթֆոններ և պլանշետներ)

• Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցներ

• Վնասաբեր հարձակումների և ծրագրերի սիգնատուրաների թարմացվող բազա

• Ռուսերեն լեզվով շահագործման ուղեցույց

Բոլոր հակավիրուսների ծրագրային ինտերֆեյսերը, ներառյալ ղեկավարման միջոցինը, պետք է լինեն ռուսերեն և անգլերեն լեզուներով:

Բոլոր հակավիրուսային միջոցները, ներառյալ ղեկավարման միջոցը, պետք է ունենան կոնտեքստային տեղեկատվական համակարգ՝ ռուսերեն և անգլերեն լեզուներով:

**Windows աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցների պահանջներ**

Windows աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

* Microsoft Windows 7
* Microsoft Windows 8
* Microsoft Windows 8.1
* Microsoft Windows 10

Windows կայանների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները.

* Հակավիրուսային սքանավորում ռեալ ժամանակում, ինչպես նաև, ըստ պահանջի, օբյեկտի կոնտեքստային մենյուից
* Նախատեսված գրաֆիկով հակավիրուսային սքանավորում
* Միացվող սարքավորումների հակավիրուսային սքանավորում
* Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
* Ակտիվ վարակվածության գործողությունների չեզոքացում
* Համակարգում ծրագրի վարքագծի և նրա կողմից ստեղծված գործողությունների վերլուծություն՝ նրա վնասակար ակտիվությունը և չարտոնված գործողությունները չեզոքացնելու համար
* Ընդհանուր կատալոգներին և ֆայլերին դիմումների վերլուծություն՝ ցանցում հասանելի պաշտպանվող ռեսուրսների գաղտնագրման փորձերը բացահայտելու համար
* Վնասակար ծրագրերի գործողությունների արգելափակում, որոնք օգտագործում են ծրագրային ապահովման խոցելիությունը, այդ թվում համակարգային գործընթացների հիշողության պաշտպանություն
* բուժման ժամանակ վնասակար ծրագրի կատարած գործողությունների հետընթացի հնարավորություն, այդ թվում վնասակար ծրագրի կողմից գաղտնագրված ֆայլերի վերականգնում
* արտոնությունների սահմանափակման հնարավորություն (գրանցում ռեեստրում, ֆայլերի, կատալոգների և այլ գործընթացների մատչում, առաջադրանքների պլանավորման դիմում, սարքավորումներին մատչելիության, օբյեկների մատչման և այլն) գործընթացների և ծրագրերի համար: Վստահության մակարդակի որոշմամբ ծրագրերի դինամիկ թարմացվող և կարգավորվող ցուցակներ:
* ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
* RAR, ARJ, ZIP, CAB, LHA, JAR, ICE ֆորմատով արխիվային ֆայլերի հակավիրուսային ստուգում և բուժում, այդ թվում գաղտնաբառով պաշտպանված:
* Հետևյալ պրոտոկոլներով աշխատող էլեկտրոնային փոստի մուտքային և ելքային հաղորդագրությունների պաշտպանություն վնասակար ծրագրերից. IMAP, SMTP, POP3, MAPI, NNTP
* փոստային կցված ֆայլերի ֆիլտր՝ տրված ֆայլերի տիպը անվանափոխելու կամ հեռացնելու հնարավորությամբ
* HTTP, FTP պրոտոկոլներով համակարգչի վրա բեռնվող թրաֆիկի ստուգում, այդ թվում էվրիստիկ վերլուծության միջոցով՝ հուսալի ռեսուրսների կարգավորման և արգելափակման ու վիճակագրության ռեժիմում աշխատելու հնարավորությամբ:
* Web էջերից ներբեռնվող բաներների և pop-up պատուհանների արգելափակում:
* Ֆիշինգային և անհուսալի կայքերի ճանաչում և արգելափակում
* Ներցանցային էկրանի առկայություն, որը թույլ է տալիս ստեղծել ցանցային փաթեթների կանոններ և ցանցային կանոններ ծրագրերի համար՝ ցանցային սեգմենտները դասակարգելու հնարավորությամբ
* Ներխուժումների հայտնաբերման և կանխարգելման համակարգի (IDS/IPS) և ցանկացած ցանցում, այդ թվում անլար, առավել հանրահայտ ծրագրերի ակտիվության ցանցային կանոնների օգտագործմամբ ցանցային գրոհներից պաշտպանություն
* ցանցային կամուրջների միջոցով կայացած ցանցային միացումների վերահսկում՝ մի քանի ցանցային կապերի միաժամանակյա միացման արգելափակման հնարավորությամբ
* բաղադրիչի առկայություն, որը թույլ է տալիս ստեղծել հատուկ կանոններ, որոնք արգելում կամ թույլ են տալիս ծրագրերի տեղադրում և/կամ գործարկումներ բոլորի կամ օգտվողների որոշակի խմբերի համար (Active Directory կամ լոկալ օգտագործողներ/խմբեր): Բաղադրիչը պետք է վերահսկի հավելվածները ինչպես ծրագրի տեղակայման ճանապարհին, մետատվյալների, վկայականի կամ մատնահետքի և MD5 կամ SHA256 ստուգման գումարի, այնպես էլ ծրագրային ապահովման արտադրողի կողմից տրամադրված նախապես որոշված կատեգորիաներով: Բաղադրիչը պետք է աշխատի սև կամ սպիտակ ցուցակի ռեժիմում, ինչպես նաև վիճակագրության հավաքման կամ արգելափակման ռեժիմում
* Օգտվողի՝ արտաքին մուտքային/ելքային սարքերի հետ աշխատանքի վերահսկում, սարքի տիպի և/կամ օգտագործվող կապուղու տիպին համապատասխան, ինչպես նաև հնարավորություն ստեղծելու վստահելի սարքերի ցուցակ ըստ դրանց իդենտիֆիկատորի, Active Directory համապատասխան օգտվողներին արտաքին սարքերի հետ աշխատելու համապատասխան առավելություն տալով:
* իրադարձությունների մատյանում շարժական կրիչների վրա ֆայլեր գրելու և/կամ ջնջելու մասին գրանցելու գրառում անելու հնարավորություն
* օգտվողի կողմից ինտերնետի հետ աշխատելու վերահսկում, այդ թվում` որոշակի բովանդակության ռեսուրսների հասանելիության բացահայտ ցուցադրման կամ թույլտվության, արտադրողի կողմից նախկինում ստեղծված և դինամիկ թարմացվող կատեգորիաների, ինչպես նաև տեղեկատվության տեսակի (աուդիո, վիդեո և այլն): Ծրագրային ապահովումը պետք է թույլ տա մուտքագրել վերահսկողության ժամանակային ինտերվալներ պարամետրեր, ինչպես նաև հանձնարարել այն միայն կոնկրետ օգտագործողներին Active Directory - ից
* BadUSB տիպի հարձակումներից պաշտպանության մեխանիզմների առկայություն
* Համակարգչի վրա տեղադրված հավելվածներում խոցելիություն հայտնաբերելու համար հատուկ մոդուլի գործարկում, որը կկարողանա ստեղծել հայտնաբերված խոցելիությունների մասին հաշվետվություն
* Սկավառակի ամբողջական կոդավորում հատուկ բեռնման մոդուլի ստեղծման և Single Sign On տեխնոլոգիայի աջակցությամբ: Օպերացիոն համակարգի ֆայլերի կամ բեռնման մոդուլի վնասման դեպքում կոդավորված պարունակության վերականգնման հնարավորությամբ գործիքներ: Պետք է գործի UEFI համակարգի հնարավորություն:
* Սկավառակի ամբողջական կոդավորման դեպքում երկֆակտոր վավերացման հնարավորություն
* Ֆայլերի կոդավորում` կոդավորվող բովանդակության ճկուն նշման ունակությամբ (տեղադրման տեղակայման միջոցով, ընդլայնման միջոցով, ֆայլ ստեղծող հավելվածի միջոցով): Ընտրված հավելվածների կողմից կոդավորված ֆայլերի հասանելիությունը սահմանափակելու մեխանիզմներ, ինչպես նաև տեխնոլոգիաների առկայություն, որը թույլ է տալիս ապակոդավորել ֆայլերը չպաշտպանված միջավայրում գաղտնաբառի միջոցով:
* Տվյալների կոդավորում շարժական կրիչների վրա, գործառնական ռեժիմը սահմանելու ունակությամբ, որը թույլ է տալիս կոդավորել և վերծանել ֆայլերը կազմակերպության ցանցից դուրս:
* Պաշտպանություն ծրագրային ծառայության չարտոնված հեռահար կառավարումից, ինչպես նաև ծրագրի պարամետրերի մատչման պաշտպանություն գաղտնաբառի միջոցով՝ վնասակար ծրագրերից, ներխուժումներից և արտոնություն չունեցող օգտվողներից
* Հակավիրուսային պաշտպանության միայն ընտրված մոդուլների տեղադրման հնարավորություն
* Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով
* Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես օպերացիոն համակարգի վերաթողարկումից հետո
* Ֆայլային տարածության սքանավորման ընթացքում համակարգչի ռեսուրսների ճկուն կառավարում՝ օգտվողներին հարմարավետ աշխատանքով ապահովելու համար
* Սքանավորման ընթացքի արագացում՝ ի շնորհիվ այն օբյեկտների սքանավորման բացառման, որոնց դրությունը նախորդ սքանավորման համեմատ փոփոխության չի ենթարկվել
* Հակավիրուսային ծրագրի ամբողջականության ստուգման հնարավորություն
* Հակավիրուսային ստուգումից բացառելու հնարավորություն ըստ ֆայլի ծավալի, դոմենի/կատալոգի դիմակի կամ ֆայլի մոտ վստահելի թվային ստորագրության առկայության
* Հակավիրուսային ծրագրում պաշտպանված պահուստարանի առկայություն՝ ջնջված վարակված ֆայլերի համար՝ դրանք վերականգնելու հնարավորությամբ
* Պաշտպանված պահուստարանի առկայություն՝ հակավիրուսի աշխատանքի հաշվետվությունների համար
* հակավիրուսի գրաֆիկական ինտերֆեյսի միացման և անջատման հնարավորություն, ինչպես նաև նվազագույն հնարավորություններով պարզեցված գրաֆիկական ինտերֆեյսի առկայություն

**Mac աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցների պահանջներ**

Mac աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

* macOS High Sierra 10.13
* macOS Sierra 10.12
* Mac OS X 10.11 (El Capitan)
* Mac OS X 10.10 (Yosemite)
* Mac OS X 10.9 (Mavericks)

Mac կայանների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները.

* Ռեզիդենտ հակավիրուսային մոնիթորինգ
* Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
* Հակավիրուսային բազաների ավտոմատ թարմացում ըստ ժամանակացույցի
* Վարակված ֆայլերի ռեզերվային պատճենում ջնջելուց առաջ ՝ դրանց հետագա վերականգնման համար
* Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
* Ներխուժումների հայտնաբերման և կանխարգելման համակարգի (IDS/IPS) և ցանկացած ցանցում, այդ թվում անլար, առավել հանրահայտ ծրագրերի ակտիվության ցանցային կանոնների օգտագործմամբ ցանցային գրոհներից պաշտպանություն
* Ֆիշինգային և վնասակար կայքերի արգելափակում հակավիրուսի արտադրողի ամպային ծառայությունների բազաներում առկա տեղեկությունների հիման վրա
* Safari, Google Chrome և Firefox բրաուզերներով փոխանցվող ինֆորմացիայի պաշտպանություն (HTTP և HTTPS թրաֆիկ)
* Սքանավորման ընթացքի արագացում՝ ի շնորհիվ այն օբյեկտների սքանավորման բացառման, որոնց դրությունը նախորդ սքանավորման համեմատ փոփոխության չի ենթարկվել
* Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով, FileVault կոդավորման ղեկավարման հնարավորությամբ

**Linux աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցների պահանջներ**

Linux աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

* Ubuntu 14.04.5, 16.04.4, 17.10.1 LTS
* Red Hat Enterprise Linux 6.9, 7.4
* CentOS-6.9, 7.4
* Debian GNU / Linux 8.10, 9.4
* OracleLinux 7.4
* SUSE Linux Enterprise Server 12 SP3
* openSUSE 42.3

Linux կայանների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

* Ռեզիդենտ հակավիրուսային մոնիթորինգ
* Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի հատուկ ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
* SMB / NFS հասանելի ռեսուրսների ստուգում
* Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
* Օգտվողի կամ ադմինիստրատորի հրամանով հակավիրուսային սքանավորում ըստ ժամանակացույցի
* zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj. արխիվներում ֆայլերի հակավիրուսային ստուգում
* տեքստային ֆորմատով էլեկտրոնային փոստի ստուգում (Plain text)
* Ֆայլերի ստուգման օպտիմիզացիայի մեխանիզմի առկայություն (բացառումներ, վստահելի ընթացքներ, ստուգման ժամանակի լիմիտավորում, ստուգվող ֆայլի ծավալի լիմիտ, ստուգված և վերջին ստուգումից հետո չփոփոխված ֆայլերի մասին տեղեկության քեշավորում)
* SMB/NFS պրոտոկոլներով ցանցային մատչումով լոկալ կատալոգներում գտնվող ֆայլերի պաշտպանություն հեռահար կոդավորումից
* Կասկածելի և վնասված օբյեկտների տեղափոխում կարանտին
* Microsoft Outlook-ի հավելվածների փոստային բազաների ստուգում
* SAMBA-ի մակարդակում ֆայլային գործընթացների ստուգման և զավթման (перехват) հնարավորություն
* Օպերացիոն համակարգի ցանցային էկրանի ղեկավարում՝ նախնական կանոնների վերականգնման հնարավորությունով
* Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես օպերացիոն համակարգի վերաթողարկումից հետո
* HTML և CSV ֆորմատներով հաշվետվությունների արտահանման և պահպանման հնարավորություն
* Ֆայլային տարածության սքանավորման ընթացքում համակարգչի ռեսուրսների ճկուն կառավարում՝ օգտվողներին հարմարավետ աշխատանքով ապահովելու համար
* Բուժումից և հեռացումից առաջ վարակված օբյեկտի կրկնօրինակի ռեզերվային պահուստարանում պահպանելու հնարավորություն՝ ցանկության դեպքում վերականգնման հնարավորությամբ, եթե տվյալ ֆայլը պարունակում է կարևոր տեղեկություն
* Առանց root իրավունքի առկայության գրաֆիկական ինտերֆեյսով ղեկավարելու հնարավորություն
* Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով

**Windows ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցների պահանջներ**

Windows ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ օպերացիոն համակարգերով աշխատող կայանների վրա.

* Windows Server 2003, 2003 R2
* Windows Server 2008, 2008 R2
* Windows Server 2012, 2012 R2
* Windows Server 2016

Windows ֆայլային սերվերների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

* Հակավիրուսային սքանավորում ինչպես ռեալ ժամանակում, այնպես էլ ըստ պահանջի տարբեր ֆունկցիաներ կատարող սերվերների վրա. Տերմինալային սերվերներ և պրինտ – սերվերներ; դոմենների կոնտրոլերների և հավելվածների սերվերներ, ֆայլային սերվերներ;
* Օգտվողի կամ ադմինիստրատորի հրամանով և ժամանակացույցով հակավիրուսային սքանավորում
* Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես օպերացիոն համակարգի վերաթողարկումից հետո
* Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի հատուկ կայքերին ՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
* RAR, ARJ, ZIP, CAB արխիվներում ֆայլերի հակավիրուսային ստուգում, այդ թվում գաղտնաբառով պաշտպանված
* Ֆայլերի, ֆայլային համակարգերի այլընտրանքային հոսքերի (NTFS-streams), բեռնման գրանցման, լոկալ և արտաքին սկավառակների բեռնման սեկտորի պաշտպանություն
* պաշտպանված սերվերի վրա Microsoft Windows Script Technologies (կամ Active Scripting) կողմից ստեղծված VBScript- ի և JScript սցենարների կատարման փորձերի շարունակական հետևում: Սկրիպտների ծրագրային կոդերի ստուգում և ավտոմատ կերպով դրանցից առավել վտանգավոր համարվողների արգելում: Հանրային թղթապանակներին և ֆայլերին դիմումների վերլուծություն, ցանցում հասանելի պաշտպանված ռեսուրսների գաղտնագրման փորձերի բացահայտում, Microsoft Windows կոնտեյներների ստուգման հնարավորություն
* ներխուժման հայտնաբերման և կանխարգելման համակարգի (IDS / IPS) միջոցով և ցանցի գործունեության կանոններով պաշտպանություն ցանցային հարձակումներից ամենատարածված ծրագրերի համար, որոնք գործում են ցանկացած համակարգչային ցանցում, ներառյալ անլար ցանցերը
* Պաշտպանել HTTP և HTTPS տրաֆիկը վիրուսներից և ֆիշինգից, ստուգելով վնասակար վեբ հասցեների հղումները և վեբ սերվերների վկայագրերի վավերականության ստուգման հնարավորությամբ ․ հղում կատարելով չարակամ վեբ հասցեների տվյալների շտեմարաններին և վեբ սերվերի վկայագրերի վավերականության ստուգման ունակությանը: Թրաֆիկի զավթում (Перехват трафика) պետք է իրականացվի զավթման դրայվերի (драйвера перехвата) օգնությամբ կամ իր վերահասցեավորման օգնությամբ:
* Բաղադրիչի առկայություն, որը թույլ է տալիս ստեղծել հատուկ կանոններ, որոնք արգելում կամ թույլ են տալիս ծրագրերի տեղադրում և/կամ գործարկումներ բոլորի համար կամ օգտվողների որոշակի խմբերի համար (Active Directory կամ լոկալ օգտագործողներ/խմբեր): Բաղադրիչը պետք է վերահսկի հավելվածները, ինչպես ծրագրի տեղակայման ճանապարհին, մետատվյալների, վկայականի կամ մատնահետքի և MD5 կամ SHA256 ստուգման գումարի: Բաղադրիչը պետք է աշխատի սև կամ սպիտակ ցուցակի ռեժիմում, ինչպես նաև վիճակագրության հավաքման կամ արգելափակման ռեժիմում: Բացի այդ, բաղադրիչը պետք է կարողանա ստեղծել թարմացումների վստահելի փաթեթների ցանկ, որոնք կարող են փոփոխել և գործարկել իրենց մեջ կցված ֆայլերը,
* Օգտվողի՝ արտաքին մուտքային/ելքային սարքերի հետ աշխատանքի վերահսկում, ինչը հնարավորություն կստեղծի կազմել վստահելի սարքերի ցուցակ և Active Directory որոշակի օգտվողներին կտա արտաքին սարքերի հետ աշխատելու առավելություն:
* Ինտերնետի հետ աշխատելու վերահսկում, ներառյալ որոշակի բովանդակությամբ ռեսուրսների հասանելության հստակ արգելումը կամ թույլտվությունը, արտադրողի կողմից նախկինում ստեղծված և դինամիկ թարմացվող կատեգորիաներին
* Ադմինիստրատորին արտաքին սարքեր միացնելու մասին տեղեկացնելը
* Ռիսկերի մեղմացման տեխնիկան օգտագործելով գործընթացների հիշողության մեջ խոցելիության շահագործման դեմ պաշտպանական մեխանիզմներ
* Սքանավորման ընթացքի արագացում՝ շնորհիվ այն օբյեկտների սքանավորման բացառման, որոնց դրությունը նախորդ սքանավորման համեմատ փոփոխության չի ենթարկվել
* Առանձին գործընթացի միջոցով սեփական մոդուլների ստուգում՝ դրանց ամբողջականության հնարավոր խախտումը հայտնաբերելու համար
* Սերվերի կարևորագույն տարածքների ստուգման կարգավորում առանձին գործընթացով
* Սերվերային ռեսուրսների բաշխում հակավիրուսային և այլ ծրագրերի միջև, կախված խնդիրների առաջնայնությունից. ֆոնային հակավիրուսային սկանավորումը շարունակելու ունակություն.
* Կարևոր իրադարձությունների մասին ադմինիստրատորներին տեղեկացնելու մի քանի ուղիների առկայություն (էլ. Փոստ, ձայնային ծանուցում, բացվող պատուհան, իրադարձությունների մատյանում գրառում)
* Ծառայությունների և հավելվածների պարամետրերին դերաբաշխված հասանելիություն թույլտվությունների ցուցակների օգնությամբ, ինչը թույլ է տալիս խուսափել վնասակար ծրագրերի, չարամիտ օգտվողների կամ անվերահսկելի օգտագործողների կողմից պաշտպանության անջատումից, ինչպես նաև արգելում կամ թույլատում է հակավիրուսի կառավարումը․
* SIEM համակարգերի հետ ինտեգրացնելու հնարավորություն
* Սարքավորումների և հավելվածների վերահսկման կանոնների ավտոմատ գեներացման մեխանիզմներ
* Հակավիրուսի աշխատանքային պռոցեսների քանակը ձեռքով առաջադրելու հնարավորություն
* Գրաֆիկական ինտերֆեյսը անջատելու կարողություն
* Լոկալ և հեռահար ղեկավարման պանելի առկայություն
* Հրամանների տողից հակավիրուսի պարամետրերի ղեկավարում
* Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով
* Օպերացիոն համակարգի ցանցային էկրանի ղեկավարում՝ նախնական կանոնների վերականգնման հնարավորությունով

**Linux ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցների պահանջներ**

Linux ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

* Ubuntu 14.04.5, 16.04.4, 17.10.1, 18.04. LTS
* Red Hat® Enterprise Linux® 6.9, 7.4
* CentOS-6.9, 7.4
* Debian GNU/Linux 8.10, 9.4
* OracleLinux 7.4.
* SUSE® Linux Enterprise Server 12 SP3.
* openSUSE® 42.3.

Linux ֆայլային սերվերների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները․

* Ռեզիդենտ հակավիրուսային մոնիթորինգ
* Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի հատուկ ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
* SMB / NFS հասանելի ռեսուրսների ստուգում
* Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ավելի արդյունավետ ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
* Օգտվողի կամ ադմինիստրատորի հրամանով հակավիրուսային սքանավորում ըստ ժամանակացույցի
* zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj. արխիվներում ֆայլերի հակավիրուսային ստուգում
* տեքստային ֆորմատով էլեկտրոնային փոստի ստուգում (Plain text)
* Ֆայլերի ստուգման օպտիմիզացիայի մեխանիզմի առկայություն (բացառումներ, վստահելի ընթացքեր, ստուգման ժամանակի լիմիտավորում, ստուգվող ֆայլի ծավալի լիմիտ, ստուգված և վերջին ստուգումից հետո չփոփոխված ֆայլերի մասին տեղեկության քեշավորում)
* SMB/NFS պրոտոկոլներով ցանցային մատչումով լոկալ կատալոգներում գտնվող ֆայլերի պաշտպանություն հեռահար կոդավորումից
* Կասկածելի և վնասված օբյեկտների տեղափոխում կարանտին
* Microsoft Outlook-ի հավելվածների փոստային բազաների ստուգում
* SAMBA-ի մակարդակում ֆայլային գործընթացների ստուգման և զավթման /перехват/ հնարավորություն
* Օպերացիոն համակարգի ցանցային էկրանի ղեկավարում՝ նախնական կանոնների վերականգնման հնարավորությունով
* Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես օպերացիոն համակարգի վերաթողարկումից հետո
* HTML և CSV ֆորմատներով հաշվետվությունների արտահանման և պահպանման հնարավորություն
* Ֆայլային տարածության սքանավորման ընթացքում համակարգչի ռեսուրսների ճկուն կառավարում՝ օգտվողներին հարմարավետ աշխատանքով ապահովելու համար
* Բուժումից և հեռացումից առաջ վարակված օբյեկտի կրկնօրինակի ռեզերվային պահուստարանում պահպանելու հնարավորություն՝ ցանկության դեպքում վերականգնման հնարավորությամբ, եթե տվյալ ֆայլը պարունակում է կարևոր տեղեկություն
* առանց root իրավունքի առկայության գրաֆիկական ինտերֆեյսով ղեկավարելու հնարավորություն
* Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով

**Շարժական սարքավորումների համար հակավիրուսային ծրագրային միջոցների պահանջներ**

Շարժական սարքավորումների / սմարտֆոների/ համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

* Android 4.2– 9.0;
* Apple iOS 9.0 – 11.4.1;

Android օպերացիոն համակարգով սմարթֆոնների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

* Սմարթֆոնի ֆայլային համակարգի մշտական հակավիրուսային պաշտպանություն՝ հակավիրուս արտադրողի հեղինակային ամպային ծառայություններում ստուգման լրացուցիչ մակարդակով
* Սմաթֆոնի ֆայլային համակարգի ստուգում ըստ պահաջի կամ ժամանակացույցի
* Տեղադրվող հավելվածների ակնթարթային ստուգում
* Ֆիշինգային և վնասակար կայքերի արգելափակում հակավիրուսի արտադրողի հեղինակային ամպային ծառայությունների բազաներում առկա տեղեկությունների հիման վրա
* Վարակված օբյեկտների մեկուսացման համար պահուստարանի առկայություն
* Վնասակար ծրագրերի որոնման և վտանգավոր օբյեկտների վնասազերծման ժամանակ օգտագործվող հակավիրուսային բազաների թարմացումներ, ըստ ժամանակացույցի
* Նշված հավելվածների թողարկման արգելափակում, այդ թվում ըստ նախապես նշված պարամետրերի: Թույլատրելի հավելվածների սպիտակ ցուցակների առկայություն
* Համակարգային հավելվածների արգելափակում
* Google Cloud Messaging-ի միջոցով անվտանգության քաղաքականությունների ստացման հնարավորություն
* Android for Work բազային աջակցում
* Բջջային ծրագրերի համար հատուկ միջավայրի ստեղծման հնարավորություն, որը կվերահսկի ծրագրերի գործողությունները, տվյալների և ծրագրային կարգավորումները ջնջելու, հավելվածի մեկնարկի համար լրացուցիչ գաղտնաբառ ավելացնելու հասանելիությամբ, այդ թվում `Active Directory- ի հավատարմագրերի օգնությամբ
* wi-fi և bluetooth մոդուլների, ինչպես նաև տեսախցիկի արգելափակման հնարավորություն
* wi-fi ցանցերին միանալու պարամետրերի ցուցումներ
* Պարտադիր տեղադրվող հավելվածների վերաբերյալ ցուցումներ տալու հնարավորություն
* Ոչ ցանկալի SMS հաղորդագրությունների արգելափակում
* Բջջային սարքի արգելափակման, տվյալների հեռացման, աշխատանքային գործունեության հետ կապված տվյալների հեռացման, սարքավորման տեղակայման կոորդինատների ստացման, գործարանային պարամետրերի հեռահար ստացման (factory reset) հնարավորություն
* Հեռախոսի կորպորատիվ քաղաքականության համապատասխանության մշտական ստուգում ավտոմատ արգելափակման հնարավորությամբ, տվյալների հեռացում, անհամապատասխանությունների դեպքում կորպորատիվ հավելվածների թողարկման արգելում
* SMS-ի միջոցով հեռախոսի ընթացիկ SIM քարտի համարի ստացում, SIM քարտի փոփոխության կամ առանց SIM քարտի հեռախոսի միացման դեպքում սարքավորման ավտոմատ արգելափակման հնարավորություն
* Samsung KNOX1 և KNOX2 տեխնոլոգիաների համատեղելիություն

Apple iOS ՕՀ համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

* Ֆիշինգային և վնասակար կայքերի արգելափակում հակավիրուսի արտադրողի հեղինակային ամպային ծառայությունների բազաներում առկա տեղեկությունների հիմքով
* Սարքավորման տեղակայման վայրի որոշման հնարավորություն

Windows Phone ՕՀ համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները․

* Ֆիշինգային և վնասակար կայքերի արգելափակում հակավիրուսի արտադրողի հեղինակային ամպային ծառայությունների բազաներում առկա տեղեկությունների հիմքով
* Սարքավորման տեղակայման վայրի որոշման հնարավորություն
* Ծրագիրը պետք է ունենա միասնական ղեկավարման վահանակից կառավարվելու հնարավորություն

**Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցների պահանջներ**

Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

* Microsoft Windows 7
* Microsoft Windows 8
* Microsoft Windows 8.1
* Microsoft Windows 10
* Windows Server 2008, 2008 R2
* Windows Server 2012, 2012 R2
* Windows Server 2016;

Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցները պետք է գործեն տվյալների բազաների կառավարման համակարգի հետևյալ տարբերակների հետ

* Microsoft SQL
* MySQL

Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

* Միասնական դիստրիբուտիվից հակավիրուսային պաշտպանության կառավարման համակարգի տեղադրում
* Պաշտպանվող հանգույցների քանակից կախված տեղադրման ընտրություն
* Active Directory-ից տեղեկության կարդացման հնարավորություն՝ կազմակերպության համակարգիչների գրանցումների և օգտվողների մասին տվյալներ ստանալու նպատակով
* Ցանցում IP հասցեի, հոսթի անվանման, դոմենի անվանման, ենթացանցի դիմակի միջոցով համակարգիչների փնտրման և հայտնաբերման հնարավորություն
* Ցանցում նոր համակարգիչների հայտնվելու դեպքում դրանց գրանցումները ըստ ղեկավարման խմբերի ավտոմատ
* Հակավիրուսային պաշտպանության ծրագրային միջոցների կենտրոնացված տեղադրում, թարմացում և հեռացում: Կենտրոնացված կարգաբերում, ղեկավարում, հաշվետվությունների և դրանց մասին վիճակագրության դիտում
* Ղեկավարման կենտրոնի միջոցով անհամատեղելի հավելվածների կենտրոնացված հեռացում (ձեռքով և ավտոմատ կերպով)
* Քաղաքականությունների և խնդիրների փոփոխությունների պատմության պահպանություն, նախորդ տարբերակներին վերադառնալու հնարավորություն
* Հակավիրուսային ագենտների տարատեսակ տեղադրման մեթոդների առկայություն. Հեռահար տեղադրման համար – RPC, GPO, ղեկավարման համակարգի միջոցով, լոկալ տեղադրման համար – տեղադրման ինքնուրույն փաթեթի ստեղծման հնարավորություն
* Անվտանգության կանոններում հատուկ թրիգերների նշման հնարավորություն, որոնք վերաբաշխում են հակավիրուսային ծրագրի կարգավորումները ըստ օգտատերերի, որից օգտագործողը մուտք է գործել, ընթացիկ IP հասցեի, ինչպես նաև կախված այն հանգամանգից , թե որ OUAD-ում է գտնվում համակարգիչը կամ որ անվտանգության խմբում է այն: Պետք է լինի հնարավորություն նման թրիգգերների խմբավորման (иерархии) համար:
* Օգտվողների համակարգչի օպերացիոն համակարգում և դրանում տեղադրված ծրագրերում խոցելիությունների ավտոմատ փնտրում և վերացում
* Նախքան հաճախորդների համակարգիչների մեջ ներբեռնված թարմացումների տարածումը՝ դրանց թեստավորումը կենտրոնացված կառավարման ծրագրային ապահովումների միջոցով․ թարմացումների տրամադրում օգտվողի աշխատատեղեր անմիջապես դրանց ստացումից հետո
* Ցանցում վիրտուալ մեքենաների ճանաչում և դրանց միջև ծանրաբեռնվածության բաշխում այն դեպքում, երբ դրանք գտնվում են նույն ֆիզիկական սերվերի վրա
* Ադմինիստրատորների և օպերատորների դերերի կարգավորման հնարավորությամբ բազմամակարդակ համակարգի ստեղծում, ինչպես նաև հաշվետվությունների տրամադրում յուրաքանչյուր մակարդակում
* Կենտրոնացված ղեկավարման համակարգի օգտվողների նախակարգաբերված դերերի առկայություն: Օգտվողների գրանցումներին կապելու նպատակով պետք է իրականացվի կոնկրետ նշված իրավասություններով դերերի խմբերի ստեղծում:
* Կամայական մակարդակի ադմինիստրավորման սերվերների հիերարխիայի ստեղծում և վերևի մակարդակից դրանց կենտրոնացված ղեկավարման հնարավորություն:
* Ղեկավարման սերվերների համար multi-tenancy աջակցություն

• Ծրագրային միջոցների և հակավիրուսային բազաների թարմացման հնարավորություն տարատեսակ աղբյուրներից, ինչպես կապուղիներով, այնպես էլ մեքենայական կրիչներից

* Կառավարման սերվերի միջոցով հակավիրուսային ԾԱ արտադրողի ամպային սերվերների մատչում
* Արտոնագրերի ավտոմատ տարածում օգտվողների համակարգիչների վրա
* Տեղակայված ծրագրային ապահովման և սարքավորումների գույքագրում օգտվողների համակարգիչների վրա
* Կառավարման կոնսոլից RDP-ի կամ կանոնավոր այլ միջոցով կապվելու հնարավորություն: Օգտագործողը պետք է հուշվի, թույլատրել հեռակա կապը:Օգտագործողին պետք է հարցում գա, հեռակա միացման վերաբերյալ:
* ՕՀ փաթեթի հետ աշխատելու գործիքակազմի առկայություն. ՕՀ փաթեթի ստեղծում ֆիզիկական կամ վիրտուալ մեքենայի հիմքի վրա, փաթեթի տեղադրում ադմինիստրատորի կողմից ընտրված համակարգիչների վրա, այդ թվում դատարկ համակարգչի (bare metal). Պետք է հնարավորություն լինի ստեղծված փաթեթում դրայվերների ցանկ ներառելու համար: ՕՀ տեղադրումից հետո սկրիպտների գործարկման կամ լրացուցիչ ԾԱ ավտոմատ տեղադրման հնարավորություն:
* Նախնական տեղադրման ծրագրակազմից ՕՀ փաթեթի ներմուծման հնարավորություն (WIM)
* Չներառված ԾԱ արտոնագրերի վերահսկման ավտոմատ համակարգի առկայություն, ադմինիստրատորին արտոնագրի օգտագործման կանոնների խախտման կամ գործողության ժամկետի ավարտի մասին տեղեկացման հնարավորությամբ:
* Չներառված հավելվածների (Adobe Reader, Mozilla Firefox, 7-zip և այլ) համար տեղադրման փաթեթների ավտոմատ ստեղծում և ավտոմատ կենտրոնացված տեղադրում համակարգիչների վրա:
* Exchange ActiveSync սերվերի միջոցով բջջային սարքերի ղեկավարման գործառույթ
* iOS MDM սերվերի միջոցով բջջային սարքերի ղեկավարման գործառույթ
* Պլանավորված/ տրված գործառույթների մասին SMS հաղորդագրությունների ուղարկման հնարավորություն
* Կառավարվող բջային սարքավորումների վրա հավելվածների կենտրոնացված տեղադրում
* Կառավարվող բջային սարքավորումների վրա արտոնագրերի կենտրոնացված տեղադրում
* Տվյալների կոդավորման գործառույթի ղեկավարման աջակցություն ունակություն
* Ղեկավարման համակարգի և ցանցի ծանրաբեռնվածությունը կանխելու համար կազմակերպության ցանկացած համակարգիչ որպես թարմացումների տարածման աղբյուր գրանցելու հնարավորություն
* Ղեկավարման համակարգի ծանրաբեռնվածությունը կանխելու համար կազմակերպության ցանկացած համակարգիչ որպես հակավիրուսային ագենտներին վերաբերվող իրադարձությունների վերահասցեավորման կենտրոն՝ ընտրված օգտատերերի համար, կառավարման կենտրոնացված համակարգին ուղարկելու աղբյուր գրանցելու հնարավորություն
* Հակավիրուսային պաշտպանության, լիցենզավորման, ինչպես նաև գույքագրման մասին գրաֆիկական հաշվետվությունների կազմում
* Համակարգի աշխատանքի վերաբերյալ նախապես կարգաբերված ստանդարտ հաշվետվությունների առկայություն
* Հաշվետվությունների արտահանում PDF և XML ֆորմատներով
* Ռեզերվային պահուստարանների և կարանտինների օբյեկտների կենտրոնացված ղեկավարում ցանցի ամբողջ ռեսուրսներում, որոնց վրա տեղադրված է հակավիրուսային ԾԱ
* Կառավարման սերվերում նույնականացման համար ներքին հաշիվների ստեղծում
* Կառավարման համակարգում ներկառուցված միջոցներով կառավարման համակարգի ռեզերվային պատճենում
* Windows Failover Clustering աջակցում
* Windows Certificate Authority ծառայության հետ ինտեգրացիայի աջակցում
* Հավելվածը կառավարելու web կոնսոլի առկայություն
* Օգտվողների ինքնասպասարկման պորտալի առկայություն: Ինքնասպասարկման պորտալը պետք է ապահովի օգտվողների միացումը հետևյալ նպատակներով. Բջջային սարքավորման վրա ղեկավարման մոդուլի տեղադրում, բջջային սարքավորումների դիտում, արգելափակման հրամանի ուղարկում, սարքավորման որոնում և բջջային սարքավորումներից տվյալների հեռացում:
* Վիրուսային համաճարակների ծագման վերահսկողության համակարգի առկայություն

**Հակավիրուսային բազաների թարմացման պահանջներ**

Թարմացվող հակավիրուսային տվյալների բազաները պետք է ապահովեն հետևյալ ֆունկցիոնալությունը.

• Կանոնավոր թարմացում առնվազն 24 անգամ օրացուցային օրվա ընթացքում:

• Թարմացման ուղիների բազմազանություն, ներառյալ կապի ուղիներով և արտաքին էլեկտրոնային սարքերով:

• Էլեկտրոնային թվային ստորագրության միջոցով թարմացումների ամբողջականության ու ինքնության ստուգում:

**Շահագործման փաստաթղթերի պահանջներ**

Բոլոր հակավիրուսային պաշտպանության ծրագրային արտադրանքների, այդ թվում` կառավարման գործիքների գործառնական փաստաթղթերը պետք է ներառեն պետական ստանդարտների պահանջներին համապատասխան պատրաստված փաստաթղթեր, ռուսերենով լեզվով, այդ թվում`

• Օգտագործման ուղեցույց (administrator).

Հակավիրուսային արտադրանքի հետ տրամադրվող փաստաթղթերը պետք է մանրամասն նկարագրեն համապատասխան հակավիրուսային պաշտպանության տեղադրման, կազմակերպման և շահագործման գործընթացը:

**Տեխնիկական աջակցման պահանջներ**

Հակավիրուսային ծրագրային ապահովման տեխնիկական աջակցությունը պետք է․

* Տրամադրվի ռուսերեն լեզվով, հակավիրուսային արտադրանք արտադրողի, նրա գործընկերների սերտիֆիկացված մասնագետների կողմից` Ռուսաստանի Դաշնության ողջ տարածքում` հեռախոսով, էլեկտրոնային փոստով և ինտերնետով:
* Արտադրողի կայքը պետք է լինի ռուսերենով, ունենա հատուկ բաժին, որը նվիրված է արտադրանքի տեխնիկական աջակցությանը, թարմացվող գիտելիքների բազա, ինչպես նաև ծրագրային արտադրանքի օգտագործողների ֆորում: