

ABSEC s.r.o.

Official AppGuard Reseller for Europe IČO: 08387508 Sídlo: Nupacká 1155/9, Strašnice, 100 00 Praha 10

Nastavení bezpečnostního subsystému pro operační systém MS Windows

Bezpečnostní subsystém je založen na bázi endpoint management aplikací AppGuard a DriveLock. Aplikace DriveLock Device Control spravuje všechna vyměnitelná média a externí zařízení, přičemž umožňuje provádět následující řízení externích médií:

- Flexibilní kontrola všech externě připojených médií, umožňuje určit, kdo a kdy může používat konkrétní externí zařízení.
- Integrovaná kontrola toku dat umožňuje definovat, kdo smí číst nebo kopírovat soubory.
- Rozsáhlý audit operací se soubory, kdy lze sledovat, kdo zkopíroval který soubor, na jaké médium a kdy to bylo provedeno.

Nastavení systému AppGuard

AppGuard zablokuje veškerý malware na úrovni jádra operačního systému, ještě než se dále rozšíří a způsobí škody.a zaručuje tzv. Zero-day ochranu tj. zabrání v den 0 spuštění úplně nových, neznámých škodlivých kódů (malwarů).

Technická specifikace

Umístění aplikace : %systemdrive%:\ProgramFiles(x86)\AppGuardLLC\AppGuard Enterprise

Typ spouštění služba Windows , AppGuardAgent.exe

Umístění auditních záznamů:

 %systemdrive%:\Program Files (x86)\AppGuard LLC\AppGuard Enterprise\egalog.log a debuglog.log Logy aktuálního dne,

Následně se tyto záznamy přesouvají v šifrované podobě do následují složky

 %systemdrive%:\Program Files (x86)\AppGuard LLC\AppGuard Enterprise\{generovane ID}, tyto auditní záznamy je možné dešifrovat pouze přenosem na centrální AGMS konzoli

Základní konifgurace AppGuardu

V případě systému AppGuard je nastavena nejpřísnější politika Workstation – Locked, kdy jsou zablokovány některé funkce Windows, například Powershell a příkazový řádek., systém umožňuje spouštění běžných aplikací, které byly v okamžiku certifikace nainstalovány v notebooku. Tuto ochranu může pozastavit pouze administrátor po zadání bezpečností hesla (Pass Phrase).



ABSEC s.r.o. Official AppGuard Reseller for Europe IČO: 08387508

Sídlo: Nupacká 1155/9, Strašnice, 100 00 Praha 10

Zapnutí Administrátorského modu (deaktivace AppGuard)

Admin mode je určen k vypnutí všech ochranných mechanizmů AppGuardu. Zapnutí admin mode se provádí přes poklepání na ikonu z oznamovací oblasti, kdy se otevře následující ovládací okno. Stisknutím tlačítka Advanced otevřeme ovládací panel pro aktivaci admin mode

Je nutné označit volby:

- Disable
- protencions
 Disable selfprotections

a vyplnit Pass Phrase¹ Vše se potvrdí tlačítkem Enable

Administrator Mode	×
Contact your AppGuard how to disable AppGuard	system administrator for instructions on d using the one-time pass phrase.
One Time Phrase:	IOPW
Pass Phrase:	
Windows Logon:	
Password:	
Disable protect	ions otection (TamperGuard) Enable Cancel

Vypnutí Administrátorského modu (aktivace AppGuard)

Stejný postup jako u zapnutí je nutné odznačit volby:

- Disable protections
- Disable self-protections

Vše se potvrdí tlačítkem Disable²¹¹.

Nastavení nové politiky

V případě nutných změn nelze novou konfiguraci vytvářet v lokálním systému. Za tímto účelem je u dodavatele udržován aktuálně platný konfigurační soubor.

V případě nutné změny jsou tyto prováděny u dodavatele, přičemž po provedné změně je tento soubor konfigurace předán bezpečnostním nebo systémovému správci.

Vlastní aplikace nastavení se provádí tak, že dodaný konfigurační soubor se nahraje do složky %systemdrive%:\ProgramData\Appguard\Policy. Nová politika se aplikuje po restartu Windows či vyvoláním volby Refresh policy.



¹ Pass Phrase je jedinečné heslo, které bylo předáno při úvodní instalaci

² Systém po startu (restartu) automaticky, bez ohledu na předchozí nastavení, startuje s vypnutým admin modem

ABSec

ABSEC s.r.o.

Official AppGuard Reseller for Europe IČO: 08387508 Sídlo: Nupacká 1155/9, Strašnice, 100 00 Praha 10

Nastavení systému DriveLock

DriveLock Device Control spravuje všechna vyměnitelná média a externí zařízení. Kontrola externích disků:

- Flexibilní kontrola všech externě připojených médií, správce určí, kdo a kdy může používat externí disky.
- Integrovaná kontrola toku dat prostřednictvím kontroly typu dat: Definujete, kdo smí číst nebo kopírovat které soubory.
- Rozsáhlý audit operací se soubory: Můžete sledovat, kdo zkopíroval který soubor. na jaké médium a kdy to bylo provedeno.

Technická specifikace

Umístění aplikace : %systemdrive%:\Program Files\CenterTools\DriveLock

Typ spouštění : služba Windows , proces DriveLock.exe

Umístění logů: využívá se integrovaný systém Windows dostupný přes Prohlížeč událostí

Konfigurace politik

Jednotlivé politiky se konfigurují pomocí správcovské konzole DriveLock Management Console



správcovská konzole DriveLock



Vytvoření politiky

Vybrat volbu Policies – horní menu Akce a dále postupovat dle obrázku Pro offline konfiguraci je nutné konfigurační soubor jako FallbackConfig.cfg

🛒 DriveL	ock - [D	riveLock\Pc	olicies]			
Soubor	Akce	Zobrazit	Nápověda			
🗢 🔿	N	lová položk	a	>	Centrally stored policy	
📑 Drivel	V	šechny úko	ly	>	Configuration file	
ြင်္ပြာ Gr	A	ktualizovat			Add Group Policy Object	
> 📴 Pc	E	xportovat s	eznam		FallbackConfig.cfg	Configu
> 📰 Dr	V	lastnosti				
>⊚Di >₿_0	N	lápověda				

postup tvorby nové politiky

Editace politiky

Příslušnou politiku lze v konzoli aplikace DriveLock editovat dvojklikem na vybraný soubor politiky, nebo přes pravé tlačítko a volbu Edit.

	Policy name		Policy type		Size	
	Sem zadejte text	Y	Sem zade	Y	Sem za	Y
ľ	FallbackConfig.cfg		Configuratio		22,5 kB	
L						



Globální nastavení agenta

V sekci Global configuration lze nastavit zásadní parametry pro běh agenta, jako jsou:

- oprávnění na ukončení agenta,
- nastavení licence
- nastavení notifikací pro uživatele.
- nastavení notifikací pro uživatele.



The DriveLock Agent contains several Windows services and device drivers. Agent self-protection lets you secure the Agent against unauthorized access, either completely, or allow access only for certain users and groups.

Do some users have local administrative rights?

Turn on non-stoppable mode to simply deny any access to DriveLock services.

Permissions on service: Default Remote control permissions: BUILTIN\Administrators Remote control permissions (readonly): No one Running in Windows Safe Mode: Disabled Running non-stoppable: Disabled Encrypted communications (SSL) enforced: Disabled

zabezpečení agenta



Zabezpečení agenta

Drivelock (vypnutí služby) je možné omezit pouze na určitou skupinu uživatelů. V případě nastavení aplikace příslušného notebooku je zvolena volba pouze pro uživatele ve skupině

"builtin\administrators"

Agent self-protection X DiveLock Agent service permissions Configure which users or groups are allowed to query, start or stop DriveLock Agent services.	\bigcirc	Agent self-protection and global security settings These settings control how DriveLock protects itself against unauthorized access to Agent services, and global security settings for Agents.
You can use this setting to prevent local administrators from stopping DirveLock services in violation of your organization's security policy. User or group Allow Deny NT AUTHORITY/SYSTEM Query service informatio BUILTIN-Administrators Full control BUILTIN-Power Users Query service informatio		 <u> Permissions on DriveLock Agent services</u> (Not configured) Configures which users or groups are allowed to query, start or stop DriveLock Agent services. You can use this setting to prevent local administrators from stopping DriveLock services in violation of your organization's security policy. <u> Run DriveLock Agent services in non-stoppable mode</u> (Disabled) Configures whether DriveLock Agent services can be stopped. You can use this setting to preven all users from stopping DriveLock services.
Add Remove Est < Zpēt Dalši > Zrušt		 Start DriveLock Agent in Safe Mode (Disabled) Configures whether DriveLock is active when the computer is running in "Safe mode". Password to uninstall DriveLock (Not configured) Configures a password that is required to uninstall the DriveLock Agent. Configure this option to prevent local administrators from uninstalling the DriveLock Agent.

Zabezpečení agenta

Nastavení správce disků

V této sekci lze povolit či zakázat připojení jednotlivých disků na základě rozhraní. V tabulce lze vidět, které rozhraní je zamčeno (Locked) či povoleno (Not locked).

Nastavení správy externích disků je založeno na principu "Blacllist" pro všechna zařízení a "WhiteList" pro schválená zařízení (zakázat vše a povolovat výjimky).

V I Drives	1	Add whitelist rule		
© Settings ■ Removable drive locking ✓ I prive whitelist rules		Removable drive locking	1	
 Windows tempore tues ✓ Windows tempore tues ✓ First type admittions ○ The type groups ○ Drive collections Ø Drive collections Ø Authorized media 		Configures the base policy used for a Start here to define how drives are co next step. Note: Bus configuration (USB, 1394, a	Il drives of a certain global type. ntrolled in your network, then create whitelist ru nd SD) takes precedence over drive type configu	les for exceptions to this basic configu
> I Devices > \rightarrow Network profiles > I and Applications		More options are available in <i>P</i> <u>Adva</u>	nced configuration	
> @ Encryption		Drive type	Status	Tasks
> 🕀 Defender Management		CD-ROM drives	Not configured (Locked)	Properties
> 🖾 Security awareness		Encrypted volumes	Not configured (Not locked)	Properties
Coperating system management Management Management coperating system		Via Firewire (1394) connected devices	Not configured (Locked)	Properties
,		Fixed disks	Not configured (Not locked)	Properties
		Floppy disk drives	Not configured (Locked)	Properties
		Network drives and shares	Not configured (Not locked)	Properties
		Other removable drives	Not locked	Properties Set to 'Not Configured'
		SD bus-connected drives	Not configured (Locked)	Properties
		Drives connected via USB	Locked	Properties Set to 'Not Configured'

globální správa externích zařízení

Kliknutím na název rozhraní lze editovat stav. Lze povolit rozhraní na základě uživatelského účtu nebo v případě volby Deny (lock for all users) lze v sekci Drive whitelist rules povolit jednotlivá

v pripade volby Deny (lock for all users) lze v sekci Drive whitelist rules povolit jednotliva zařízení.

ABSec

ABSEC s.r.o.

Official AppGuard Reseller for Europe IČO: 08387508 Sídlo: Nupacká 1155/9, Strašnice, 100 00 Praha 10

Přidání nového zařízení

Drive whitelist rules			
🖄 Whitelist temp	Nová položka	>	Drive rule
S File filter template	Všechny úkoly	>	Drive collection rule
 File type defini File type group Drive collections Authorized media Devices Network profiles 	Zobrazení Otevřít v novém okně Exportovat seznam Vlastnosti	>	Network drives rule WebDAV-based network drives rule Drive size rule Encrypted media rule Base rule
Applications	Nápověda		Terminal services rule
Defender Management			Rule from template
Security awareness			Hardware ID rule
Inventory and vulnerabilit Operating system manage	y scan ement		Folder

Přidání nového zařízení

- 1) Pravé tlačítko na položku menu
- 2) Výběr zařízení na základě připojených zařízení k danému počítači
- 3) Pro povolení zařízení musí být vybrána volba Active

Zároveň musí být nastavena volba omezení na základě sériového čísla (volba Only allow selected serial numbers)

New drive exceptior	– vlastnosti			?	×	<
Logged on users	Drive letters	Awaren	ess	М	essages	
Encryption	Options	B Drive scan		Con	nmands	
General Permission	s Filter / Shadow	w Time limits Comp		uters	Network	s
Vendor ID						L
Product ID					-	
Active						_
Comment]
Symbol 😞	~					
	d and d an order and					
	d senal numbers					
Serial number	Comment			A	dd	
				Re	emove	
					da	i.
					.un	
	01		×		D 14	
	OK	Zn	Jšít		Použít	

Logge	d on users		Drive lette	rs	Awaren	ess	M	essages
Encry	ption	0	otions	ions Drive scan			Com	imands
General	Permissio	ns F	lter / Shad	ow	Time limits	Com	puters	Networks
Hardware	e ID USE	BSTOR	\Disk Kings	ston[)ataTraveler	_2.0P	MAP	
This type Disk Veno endpoint	of rule is b dor_Produc security so	ased o ct'') and lutions	n the Wind is provide to DriveLo	dows dma ck.	hardware IE inly for upgra) (e.g. ading f	"USBS rom oth	iTOR∖ ler
Active	e							
Comment	t king	ston						
	allow select	√ ted ser	ial numbers	3				
Ser	ial number		Comment				A	dd
c.84	50008863F	7506						
	0000000						Re	move
							E	dit



Aplikace politiky



- 2) Zavřít okno politiky
- Kopírovat uložený soubor FallbackConfig.cfg do systémové složky Drivelock - C:\Program Files\CenterTools\DriveLock (přepsat stávající soubor)

Do umístění souboru s konfigurací se lze dostat například z okna hlavní konzole pomocí následující volby

4) Restartovat službu DriveLock



Antivirová ochrana

K zajištění této funkcionality bude využíván program Windows Defender, který představuje klasický antivirový program v kombinaci se systémem AppGuard (viz předchozí bod)

U KPS bylo rozhodnuto, že offline aktualizace antivirových definic nebude prováděna. Bezpečnostní správce informačního systému má za to, že větší riziko, vzhledem ke konfiguraci notebooku představuje tato aktualizace než její neprovedení.

- Bezpečnostní správce / správce informačního systému zajistí, aby rezidentní část antivirového software byla aktivována při startu notebooku a pracovala při jeho běhu. Rezidentní ochrana notebooku bude zapnuta, a to včetně testování SSD a USB flash pamětí.
- V případě, že je nalezen vir, je oprávněn jej odstranit správce informačního systému. Uživatel, který vir zjistil, neprodleně o této skutečnosti informuje Bezpečnostního správce informačního systému. Bezpečnostní správce informačního systému pak zajistí v součinnosti se správcem informačního systému provedení kompletních antivirových testů na všech nosičích utajovaných informací, které byly od poslední kompletní kontroly používány. V případě, že infikovaná data pocházejí od jiného subjektu, informuje Bezpečnostní správce informačního systému daný subjekt o zjištěném viru.

Vzhledem k instalované technologii AppGuard lze konstatovat, že vir se z případně nakaženého souboru vzhledem k "sandboxování" nebude v informačním systému šířit dále.